# On the use of the 2-D cyclic structure of cyclic codes

**Eindhoven University of Technology**
**Department of Mathematics and Computing Science**

Master's Thesis

# On the Use of the 2-D Cyclic Structure of Cyclic Codes

by

P.J.N. de Rooij

**EUT Report 90-WSK-03**

**Eindhoven December 1990**

Department of Mathematics and Computing Science
Eindhoven University of Technology
P.O. Box 513
5600 MB Eindhoven, The Netherlands
ISSN 0167-9708
Coden: TEUEDE

# On the Use of the 2-D Cyclic Structure of Cyclic Codes

by

P.J.N. de Rooij

## Abstract

This report deals with the 2-D cyclic structure of cylic codes of composite length, and the use of this structure. A bound of the minimum distance of the code can be derived from this structure, but it is proved that in general this bound (the Jensen Bound, cf. [3]), is not very good (compared to shifting). With the use of the 2-D cyclic structure, however, the exact minimum distance of two codes, for wich this had not been done before, hase been found. Finally, some good codes are constructed with use of their 2-D cyclic structure.

**AMS (MOS) subject classification** 94B15

# Preface

This report is an improved version of my Master's Thesis [11] at Eindhoven University of Technology. Compared to this thesis, only minor changes are made. A few typing errors and some incorrect sentences were corrected, some superfluous paragraphs were deleted and the appendix was left out.

Most importantly, however, some of the proofs in Chapter 3 are shortened. For this, and for the help with and editing of our joint paper [12], I would like to thank prof. van Lint. Furthermore, he provided much more elegant proofs (compared to the ones I came up with) for the main results of Chapter 3, for which I am grateful too. (These proofs are already included in [11].) Finally, the choice of subject for the master's thesis was inspired by his treatment of J. M. Jensen's paper [3].

# Contents

# Introduction

This report deals with the 2-D cyclic structure of cyclic codes of composite length, and with the use of this structure in estimating the minimum distance of those codes.

Chapter 1 introduces the concept of 2-D cyclic codes, and is an adaptation of the article by J. M. Jensen ([3]), where it was first shown that every 2-D cyclic code can be decomposed in a direct sum of several concatenated codes, with minimal cyclic inner and cyclic outer codes, and, conversely, that a 2-D cyclic code can be constructed this way. Berlekamp and Justesen have shown, in [1], that such a direct sum of concatenated codes is equivalent to a cyclic code, whenever the lengths of the inner and outer codes are relatively prime.

Furthermore an estimate for the minimum distance of such a (2-D) cyclic code is derived. This bound is called the Jensen Bound.

In Chapter 2 the performance of this bound is evaluated. This is done by comparing it to shifting, which in general yields the best known bounds. For this purpose a theorem is proved, stating that, under certain assumptions, the bound provided by shifting is at least as good as the Jensen Bound. For all binary cyclic codes of length 63 these assumptions are satisfied; and for 'good' codes of this length shifting indeed performs much better.

Furthermore a criterion on when the Jensen Bound is sharp is derived. This criterion proves to be of some interest with respect to the judgement of the performance of the Jensen Bound.

We can conclude that in general, the Jensen Bound will not be a very powerful tool in the determination of the minimum distance of cyclic codes.

In Chapter 3, however, we see that the 2-D cyclic structure of a cyclic code reveals some useful information on words of minimum distance. In that respect the Jensen Bound proves to be very useful, for it is one of the (necessary) tools in the determination of the minimum distance of two codes that (to the knowledge of the author) had resisted all earlier attempts (except computer search) using other methods.

Finally, some codes are constructed with the use of 2-D cyclic structure.

We do not consider the use of the 2-D cyclic structure of cyclic codes for decoding purposes. For this subject we refer to [14].

# Chapter 1

# 2-D cyclic codes

## 1.1 Introduction

In this chapter 2-D cyclic codes are introduced. We show that a 2-D cyclic code can be decomposed into the direct sum of a number of concatenated codes—with primitive cyclic inner codes and cyclic outer codes.

Furthermore we show that a $q$-ary cyclic code of length $nN$ with $\gcd(nN, q) = \gcd(n, N) = 1$ can be seen as a 2-D cyclic code. From the decomposition of the 2-D cyclic code we then find a lower bound on the minimum distance of the cyclic code —the Jensen Bound.

## 1.2 Definitions

Let $G$ be an Abelian group of order $nN$ that is the direct product of two cyclic subgroups $G_x$ and $G_y$ of order $n$ respectively $N$. That is, $G = G_x \times G_y$ contains (say) the elements $\{x^i y^j \mid 0 \leq i < n \ \wedge \ 0 \leq j < N\}$, $(x^n = y^N = 1)$. Let $q$ be a prime power and $\gcd(nN, q) = 1$.

**Definition 1.2.1** *The* group algebra $\mathsf{F}_q G$ *is the ring (with unity) consisting of all (formal) polynomials*

$$c(x, y) = \sum_{i=0}^{n-1} \sum_{j=0}^{N-1} c_{ij} x^i y^j, \text{ where } c_{ij} \in \mathsf{F}_q.$$

Addition and multiplication in $\mathsf{F}_q G$ are defined in the obvious way:

$$c(x, y) + d(x, y) = \sum_{i=0}^{n-1} \sum_{j=0}^{N-1} (c_{ij} + d_{ij}) x^i y^j$$

and

$$c(x, y) \cdot d(x, y) = \sum_{i=0}^{n-1} \sum_{j=0}^{N-1} \Big( \sum_{\substack{i_1 + i_2 \equiv i \\ j_1 + j_2 \equiv j}} c_{i_1 j_1} d_{i_2 j_2} \Big) x^i y^j,$$

where $c, d \in \mathbb{F}_q G$ and $i_1, i_2 \in \mathbb{Z}_n$ and $j_1, j_2 \in \mathbb{Z}_N$.

**Definition 1.2.2** *An* ideal $\mathcal{I}$ *in a ring* $\mathcal{R}$ *is a nonempty subset of* $\mathcal{R}$ *satisfying:*

1. *If* $a, b \in \mathcal{I}$ *then* $a - b \in \mathcal{I}$.
2. *If* $a \in \mathcal{I}$ *and* $r \in \mathcal{R}$ *then* $ra \in \mathcal{I}$.

**Definition 1.2.3** *A* 2-D cyclic code *over* $\mathbb{F}_q G$ *is an ideal in* $\mathbb{F}_q G$.

We represent a codeword by the corresponding polynomial or by the $n \times N$ matrix $\|c_{ij}\|$. We will not distinguish these notations, not even in maps and functions etc.

**Corollary 1.2.4** *A 2-D cyclic code over* $\mathbb{F}_q G$ *is invariant under cyclic permutation of rows and columns (in the matrix representation); we call this* rowcyclic *respectively* columncyclic.

**Proof:** Multiplication by the polynomials $x$ and $y$ shifts the rows respectively columns of the matrix representation of a codeword cyclically over 1 position. □

Now we easily see the following.

**Corollary 1.2.5** *A nonempty subset* $\mathcal{C} \subseteq \mathbb{F}_q G$ *satisfying*

1. *if* $a, b \in \mathcal{C}$ *and* $\lambda, \mu \in \mathbb{F}_q$ *then* $\lambda a + \mu b \in \mathcal{C}$ *(i.e.,* $\mathcal{C}$ *is linear);*
2. $\mathcal{C}$ *is row- and columncyclic;*

*is 2-D cyclic.*

**Proof:** From 2. follows $x\mathcal{C} = \mathcal{C}$ and $y\mathcal{C} = \mathcal{C}$, so $x^i y^j \mathcal{C} = \mathcal{C}$; with 1. we even find $f(x, y)\mathcal{C} = \mathcal{C}$ for all $f \in \mathbb{F}_q G$. This means that $\mathcal{C}$ satisfies the second requirement in Definition 1.2.2. The first requirement is easily seen to follow from 1. □

If $\gcd(n, N) = 1$, then the Chinese Remainder Theorem provides a unique $\mu \in \{0, 1, \ldots, nN - 1\}$ for every $i, j$ $(0 \leq i < n, 0 \leq j < N)$, such that $\mu \equiv i \pmod{n}$ and $\mu \equiv j \pmod{N}$. Defining $Z = xy$ we conclude that this $\mu$ satisfies $Z^\mu = x^i y^j$. Now every element of $G$ is a power of $Z$, and $Z$ has order $nN$, so $G$ is cyclic. (Of course there are more generators in $G$, but $Z$ proves to be a suitable choice for our purposes.) Knowing this, we can state the following.

**Corollary 1.2.6** *If* $\gcd(n, N) = 1$, $G$ *and* $q$ *as above, then a 2-D cyclic code* $\mathcal{C} \in \mathbb{F}_q G$ *is cyclic.*

**Proof:** $C$ is linear (for it is an ideal in $\mathsf{F}_q G$), $ZC = C$ and $Z$ has order $nN$. □

The reverse of this result holds as well.

**Corollary 1.2.7** *A cyclic code of length $nN$, with $\gcd(n, N) = 1$ is 2-D cyclic.*

**Proof:** Let $Z = xy$, where codewords of the cyclic code are polynomials in $Z$ and $x$ and $y$ are primitive $n$th and $N$th roots of unity, respectively. Now $Z^\mu = x^i y^j$, where $i \equiv \mu \pmod{n}$ and $j \equiv \mu \pmod{N}$. Because the Chinese Remainder Theorem provides a bijection $\{0, 1, \ldots, nN-1\} \to \{0, 1, \ldots, n-1\} \times \{0, 1, \ldots, N-1\}$, we can represent every codeword as a matrix. This matrix form of the code is row- and columncyclic, for $x$ and $y$ are powers of $Z$, and $Z^\mu C = C$. $C$ trivially is linear. □

## 1.3 Concatenation

We can describe the concept of concatenation of codes as follows[1]. A first code $\mathcal{B} \subseteq \mathsf{F}_{q^k} G_y$ —the so-called *outer code*—is used to encode the information. Next, the letters of this code are as it were inflated by sending not the letter itself, but a codeword from a second code $\mathcal{A}$ —the so-called *inner code*. The receiver first retrieves the letters in $\mathsf{F}_{q^k} G_y$ from those words in $\mathcal{A}$, then the word in $\mathcal{B}$ is decoded.

A word emerging from the inner encoder consists of a row of codewords of $\mathcal{A}$. We can place these words as columns in a matrix. If we want to make a 2-D cyclic code this way, we must require a number of things of $\mathcal{A}$ and $\mathcal{B}$: obviously $\mathcal{A}$ and $\mathcal{B}$ must be cyclic, and $\mathcal{A}$ must be a code over $\mathsf{F}_q$. Furthermore, a necessary condition of course is that the map $\mathsf{F}_{q^k} \to \mathcal{A}$ is injective; so $\mathcal{A}$ must have at least $q^k$ words. This map also should satisfy some conditions, for example that a cyclic shift of the words in the inner code corresponding to letters of a codeword does something to these letters that makes the resulting word a codeword.

We do not go into this any further (see [8] for more details) and give the construction from [3].

Let $\mathcal{A}_s$ be a minimal cyclic code of dimension $k$ in $\mathsf{F}_q G_x$,[2] and $\mathcal{B}$ a cyclic code of dimension $K$ in $\mathsf{F}_{q^k} G_y$. We must find a bijection $\mathcal{A}_s \leftrightarrow \mathsf{F}_{q^k}$ such that the concatenation $\mathcal{A}_s \square \mathcal{B}$ is an ideal in $\mathsf{F}_q G$. We choose the isomorfism $\phi_s : \mathcal{A}_s \to \mathsf{F}_{q^k}$ given by $\phi_s(a(x)) = a(\beta_s)$, where $\beta_s$ is a nonzero of the generator of $\mathcal{A}_s$.

Trivially, $\phi_s$ is a homomorfism; we show now that $\phi_s$ is bijective too. Suppose $\phi_s(a(x)) = \phi_s(b(x))$, $a, b \in \mathcal{A}_s$. Then $a(\beta_s) = b(\beta_s)$. From this we find $a(\beta_s^q) = b(\beta_s^q), a(\beta_s^{q^2}) = b(\beta_s^{q^2}), \ldots, a(\beta_s^{q^{k-1}}) = b(\beta_s^{q^{k-1}})$, so $a(x) = b(x)$ for all nonzeros of the generator of $\mathcal{A}_s$. For the zeros of this generator of course the same holds,

[1] We give a special case of the Blokh-Zyablov construction; we do not complicate matters more than necessary for our purposes; see [2].

[2] In other words, $\mathcal{A}_s \subseteq \mathsf{F}_q[x]/(x^n - 1)$.

so we may conclude $\{a-b\}(x)=0$ for all $n$th roots of unity, so $a=b$, since $\deg(a-b)<n$. Apparently $\phi_s$ is injective, and because $|\mathcal{A}_s|=|\mathbb{F}_{q^k}|$ it even is bijective, so it is an isomorfism.

The inverse $\psi_s$ of $\phi_s$ is defined by:

$$\psi_s(\delta)=\sum_{i=0}^{n-1}\frac{1}{n}\mathrm{Tr}_k(\delta\beta_s^{-i})x^i \text{ for } \delta\in\mathbb{F}_{q^k}.$$

Here $\mathrm{Tr}_k$ is the tracefunction $\mathbb{F}_{q^k}\to\mathbb{F}_q$: $\mathrm{Tr}_k(\delta)=\delta+\delta^q+\cdots+\delta^{q^{k-1}}$. Indeed we see

$$\begin{aligned}\phi_s(\psi_s(\delta)) &= \sum_{i=0}^{n-1}\frac{1}{n}\mathrm{Tr}_k(\delta\beta_s^{-i})\beta_s^i\\ &= \sum_{i=0}^{n-1}\frac{1}{n}\sum_{j=0}^{k-1}\delta^{q^j}\beta_s^{(1-q^j)i}\\ &= \sum_{j=0}^{k-1}\frac{1}{n}\delta^{q^j}\sum_{i=0}^{n-1}\beta_s^{(1-q^j)i}\\ &= \delta,\end{aligned}$$

for the inner sum (in the last row but one) equals 0 if $\beta_s^{1-q^j}\neq 1$, that is, if $j\neq 0$, and equals $n$ otherwise.

Furthermore, note that $\psi_s(1)$ exactly equals the idempotent $\theta_s(x)$ of $\mathcal{A}_s$, since $(\psi_s(1))^2=\psi_s(1^2)=\psi_s(1)$, and $\psi_s(1)\cdot a(x)=\psi_s(1)\cdot\psi_s(\phi_s(a(x)))=\psi_s(1\cdot\phi_s(a(x)))=a(x)$ for all $a\in\mathcal{A}_s$. From this we also find: $\phi_s(\lambda\theta_s(x))=\lambda\theta_s(\beta_s)=\lambda\phi_s(\theta_s(x))=\lambda$ and even $\phi_s(\lambda a(x))=\lambda\phi_s(a(x))$ for all $\lambda\in\mathbb{F}_q$.

Let $(\boldsymbol{a}_0,\boldsymbol{a}_1,\ldots,\boldsymbol{a}_{N-1})\in\mathcal{A}_s\Box\mathcal{B}$, where the $\boldsymbol{a}_j$ are columnvectors[3] of length $n$ over $\mathbb{F}_q$. Then $\boldsymbol{a}_j\in\mathcal{A}_s$ for all $j$, and $(a_0(\beta_s),a_1(\beta_s),\ldots,a_{N-1}(\beta_s))\in\mathcal{B}$. Now perform a cyclic shift over one position with the rows of the matrix representation of this word, that is, the entries within each column are simultaneously shifted over one position. Then we find the columns represented by the polynomials $xa_j(x)$. All these are words from $\mathcal{A}_s$, so we may apply $\phi_s$ to all columns. Doing this we see that these words in $\mathcal{A}_s$ correspond to $\beta_s$ times the old letter. So our shifted word corresponds to a word in $\mathcal{B}$. In other words: we have obtained a word in $\mathcal{A}_s\Box\mathcal{B}$, so $\mathcal{A}_s\Box\mathcal{B}$ is rowcyclic. $\mathcal{A}_s\Box\mathcal{B}$ is columncyclic because $\mathcal{B}$ is cyclic.

Finally, we show that $\mathcal{A}_s\Box\mathcal{B}$ is linear. Let $\lambda,\mu\in\mathbb{F}_q$ and $\boldsymbol{a}=(\boldsymbol{a}_0,\ldots,\boldsymbol{a}_{N-1})$, $\boldsymbol{b}=(\boldsymbol{b}_0,\ldots,\boldsymbol{b}_{N-1})\in\mathcal{A}_s\Box\mathcal{B}$, (i.e., $\boldsymbol{a}_i\in\mathcal{A}_s,(\phi_s(\boldsymbol{a}_0),\ldots,\phi_s(\boldsymbol{a}_{N-1}))\in\mathcal{B}$ and analogously for $\boldsymbol{b}_i$.) Now $\lambda\boldsymbol{a}_i+\mu\boldsymbol{b}_i\in\mathcal{A}_s$ for all $i$, and $\phi_s(\lambda\boldsymbol{a}_i+\mu\boldsymbol{b}_i)=\lambda\phi_s(\boldsymbol{a}_i)+\mu\phi_s(\boldsymbol{b}_i)$, so $(\phi_s(\lambda\boldsymbol{a}_0+\mu\boldsymbol{b}_0),\ \ldots,\ \phi_s(\lambda\boldsymbol{a}_{N-1}+\mu\boldsymbol{b}_{N-1}))=\lambda\Phi(\boldsymbol{a})+\mu\Phi(\boldsymbol{b})\in\mathcal{B}$. Therefore $\lambda\boldsymbol{a}+\mu\boldsymbol{b}\in\mathcal{A}_s\Box\mathcal{B}$. This proves the following theorem.

[3]We use boldface to indicate vectors, the corresponding italics for the corresponding polynomials.

**Theorem 1.3.1** *If $\mathcal{A}_s$ is a minimal cyclic code of dimension $k$ in $\mathsf{F}_q$, $\mathcal{B}$ is a cyclic code of dimension $K$ in $\mathsf{F}_{q^k}G_y$ and $\phi_s$ and $G$ are as above, then $\mathcal{A}_s\Box\mathcal{B}$ is a 2-D cyclic code (of dimension $kK$) in $\mathsf{F}_qG$.*

We summarize this construction in the following notation (where $\Psi_s$ denotes the map that maps a word in $\mathcal{B}$ to a matrix in $\mathcal{A}_s\Box\mathcal{B}$).

$$\Psi_s(b(y)) = \Psi_s\left(\sum_{j=0}^{N-1} b_j y^j\right) = \sum_{j=0}^{N-1} \psi_s(b_j)y^j \ , \ b(y) \in \mathsf{F}_{q^k}G_y.$$

$\Psi_s$ is an injective homomorfism $\mathsf{F}_{q^k}G_y \rightarrow \mathsf{F}_qG$, as $\psi_s$ is an injective homomorfism $\mathsf{F}_{q^k} \rightarrow \mathsf{F}_qG_x$.

The inverse map $\Phi_s$ of $\psi_s$ is defined as

$$\begin{aligned}\Phi_s(c(x,y)) &= \Phi_s\left(\sum_{j=0}^{N-1}\sum_{i=0}^{n-1} c_{ij}x^i y^j\right) \\ &= \sum_{j=0}^{N-1} \phi_s\left(\sum_{i=0}^{n-1} c_{ij}x^i\right) y^j, \quad c \in \Psi_s(\mathsf{F}_{q^k}G_y).\end{aligned}$$

## 1.4 Decomposition of 2-D cyclic codes

In this section we show that a 2-D cyclic code in $\mathsf{F}_qG$ can be decomposed in a unique way into the direct sum of concatenated codes $\mathcal{A}_s\Box\mathcal{B}$ as in the preceding section.

We have several codes $\mathcal{A}_s$ now—so we have several fields $\mathsf{F}_{q^k}$ too. Therefore, the field $\mathsf{F}_{q^k}$ corresponding to $\mathcal{A}_s$ will be denoted as $F_s$ in the sequel. The related code $\mathcal{B}$ will get an index $s$ as well.

For the primitive idempotents $\theta_s$ of the (minimal) cyclic codes over $\mathsf{F}_q$ the following holds: $\mathsf{F}_qG_x = \bigoplus_{s=1}^{v}\langle\theta_s\rangle$, $\sum_{s=1}^{v}\theta_s = 1$, $\theta_s \cdot \theta_s = \theta_s$ and $\theta_{s_1} \cdot \theta_{s_2} = 0$ if $s_1 \neq s_2$. We do something similar now for 2-D cyclic codes. First, we define the 2-D-analogue of an idempotent in a cyclic code.

**Definition 1.4.1** $\Theta_s = \Psi_s(1)$, *where* 1 *is the unity in* $F_sG_y$. *This is an* idempotent *in* $\mathsf{F}_qG$.

Notice that $\Theta_s$ in matrix form has $\theta_s$ as its first column, and further consists of zero columns only. We now prove that $\Theta_s$ indeed is worthy of the name idempotent. It is, by the way, not a *primitive* idempotent.

**Theorem 1.4.2** *If* $\mathsf{F}_qG_x = \bigoplus_{s=1}^{v}\langle\theta_s\rangle$, *then*

1. $\mathsf{F}_qG = \bigoplus_{s=1}^{v}\langle\Theta_s\rangle$, *where* $\langle\Theta_s\rangle = \Psi_s(F_sG_y)$;

2. $\Theta_s \cdot \Theta_s = \Theta_s$ *for all* $s$; $\Theta_{s_1} \cdot \Theta_{s_2} = 0$ *for* $s_1 \neq s_2$;

3. $\sum_{s=1}^{v} \Theta_s = 1$.

**Proof:** 1. It is easy to see that $\langle \Theta_s \rangle = \Psi_s(F_s G_y)$ and consists exactly of those matrices in the matrix representation of $\mathbb{F}_q G$ of which all columns are words of $\langle \theta_s \rangle$.

From this it easily follows that $\sum_{s=1}^{v} \langle \Theta_s \rangle = \mathbb{F}_q G$. So the only thing left to prove is that this sum is direct. We do this by showing the following: if $\sum_{s=1}^{v} c_s(x,y) = 0$ (where $c_s(x,y) \in \langle \Theta_s \rangle$ ), then $c_s(x,y) = 0$ holds for all $s$.

So let $\sum_{s=1}^{v} c_s(x,y) = 0$ and $c_s(x,y) = \sum_{j=0}^{N-1} \psi_s(b_{sj}) y^j \in \langle \Theta_s \rangle$. Then it follows that $\sum_s \sum_j \psi_s(b_{sj}) y^j = 0$, so $\sum_{s=1}^{v} \psi_s(b_{sj}) = 0$ for $j = 0, 1, \ldots, N-1$. Now $\psi_s(b_{sj}) \in \langle \theta_s \rangle$ for all $s$ and $j$; and we have $N$ equations in $\mathbb{F}_q G_x$. Since $\mathbb{F}_q G_x$ equals the *direct* sum of the $\langle \theta_s \rangle$, $s = 1, 2, \ldots, v$, we have $\psi_1(b_{1j}) = \psi_2(b_{2j}) = \ldots = \psi_v(b_{vj}) = 0$ for all $j$, $0 \leq j < N$.

2. If we consider $\Theta_{s_1}$ and $\Theta_{s_2}$ as polynomials, we see that $\Theta_{s_1} \cdot \Theta_{s_2} = \theta_{s_1} \cdot \theta_{s_2}$. This proves 2.

3. Analogously it follows that $\sum_{s=1}^{v} \Theta_s = \sum_{s=1}^{v} \theta_s = 1$. □

This has provided us with the tools to prove the announced Decomposition Theorem.

**Theorem 1.4.3** *Let* $\mathcal{C} \subseteq \mathbb{F}_q G$ *be a 2-D cyclic code. Then the following holds:*

1. $\mathcal{C} = \bigoplus_{s \in I} \mathcal{C}_s$, *where* $\mathcal{C}_s = \mathcal{C} \cdot \Theta_s \subseteq \langle \Theta_s \rangle$ *for all* $s$ *and* $I = \{s \mid \mathcal{C}_s \neq 0\}$;

2. $\mathcal{C}_s = \langle \theta_s \rangle \square \mathcal{B}_s$, *where* $\mathcal{B}_s = \Phi_s(\mathcal{C}_s)$.

**Proof:** $\mathcal{C}$ is a 2-D cyclic code, so $\mathcal{C} = \mathcal{C} \cdot 1 = \mathcal{C} \cdot \sum_{s=1}^{v} \Theta_s = \bigoplus_{s=1}^{v} \mathcal{C} \cdot \Theta_s = \bigoplus_{s=1}^{v} \mathcal{C}_s$. This sum is direct, for $\mathcal{C} \cdot \Theta_s \subseteq \mathbb{F}_q G \cdot \Theta_s = \langle \Theta_s \rangle$. This shows us that $\mathcal{C}_s \subseteq \Psi_s(F_s G_y)$, which implies that $\mathcal{B}_s \stackrel{\text{def}}{=} \Phi_s(\mathcal{C}_s)$ is a cyclic code in $F_s G_y$. Finally, $\langle \theta_s \rangle \square \mathcal{B}_s = \langle \theta_s \rangle \square \Phi_s(\mathcal{C}_s) = \mathcal{C}_s$ as a consequence of the definitions of $\Phi_s$ and concatenation. □

In this way we can *construct* a 2-D cyclic code too, as follows from the next theorem.

**Theorem 1.4.4** *Let there be given a number of minimal cyclic codes* $\langle \theta_s \rangle$ *of dimension* $k_s$ *in* $\mathbb{F}_q G_x$ *and cyclic codes* $\mathcal{B}_s$ *in the related fields* $F_s$, $s \in I$. *Then* $\mathcal{C} = \bigoplus_{s \in I} \langle \theta_s \rangle \square \mathcal{B}_s$ *is a 2-D cyclic code of dimension* $\sum_{s \in I} k_s \cdot \dim(\mathcal{B}_s)$.

**Proof:** The sum of a number of ideals is an ideal, so $\mathcal{C}$ is a 2-D cyclic code. Since $\langle \theta_s \rangle \square \mathcal{B}_s \subseteq \langle \Theta_s \rangle$ the sum is direct (see Theorem 1.4.2). The dimension follows immediately from Theorem 1.3.1 and the definition of direct sum. □

## 1.5 The Jensen Bound

For a code $\mathcal{A}_s \Box \mathcal{B}$, we easily find a lower bound on the minimum distance. Let $d_1$ and $d_2$ be the minimum distances of $\mathcal{A}_s$ respectively $\mathcal{B}$. Then $\mathcal{A}_s \Box \mathcal{B}$ has at least $d_2$ nonzero columns, all of which have weight at least $d_1$. So the minimum distance $d_{\min}$ of the concatenated code satisfies $d_{\min} \geq d_1 d_2$.

We apply this idea to an arbitrary 2-D cyclic code $\mathcal{C} = \bigoplus_{s \in I} (\langle \theta_s \rangle \Box \mathcal{B}_s)$, where $\mathcal{B}_s \subseteq F_s G_y$. Denote the minimum distances of the composing codes as follows: $d_{1l} = d_{\min}\left(\bigoplus_{s \in I, s \leq l} \langle \theta_s \rangle\right)$, $d_{2l} = d_{\min}(\mathcal{B}_l)$.

Take a word $\boldsymbol{c} \in \mathcal{C}$ of minimum weight, say $\boldsymbol{c} = \sum_{s \in I} \boldsymbol{c}_s$, where $\boldsymbol{c}_s \in \langle \theta_s \rangle \Box \mathcal{B}_s$. Now let $l = \max\{s \in I \mid \boldsymbol{c}_s \neq \boldsymbol{0}\}$. Analogous to the argument above, we find that $\boldsymbol{c}$ has at least $d_{2l}$ nonzero columns. Each of these columns is an element of $\bigoplus_{s \in I, s \leq l} \langle \theta_s \rangle$, so each of them has weight at least $d_{1l}$. With this we find the following theorem.

**Theorem 1.5.1** *Let $\mathcal{C} = \bigoplus_{s \in I} (\langle \theta_s \rangle \Box \mathcal{B}_s)$ with $\mathcal{B}_s \subseteq F_s G_y$ for all $s \in I$. Then the minimum distance $d$ of $\mathcal{C}$ satisfies:*

$$d \geq \min\{d_{1l} d_{2l} \mid l \in I\} \tag{1.1}$$

The value of $d$ in this theorem still depends on the numbering of the idempotents $\theta_s$ (and, as we will see in Section 2.2, not on the choice of the $\beta_s$). We find the maximal value using the numbering of the $\theta_s$ that satisfies $d_{21} \leq d_{22} \leq \cdots \leq d_{2 s_{\max}}$, where $s_{\max} = \max\{s \mid s \in I\}$.
Proof of this claim: let $d_{2l} > d_{2,l+1}$. If we interchange these two, only the terms $d_{1l} d_{2l}$ and $d_{1,l+1} d_{2,l+1}$ change. Using a somewhat sloppy notation —where $d'_{1l} = d_{\min}\left(\left(\bigoplus_{s \leq l-1} \langle \theta_s \rangle\right) \oplus \langle \theta_{l+1} \rangle\right) > d_{1,l+1}$— this boils down to

$$\begin{aligned} d_{1l} d_{2l} \mapsto d'_{1l} d_{2l+1} &> d_{1,l+1} d_{2,l+1}, \\ d_{1,l+1} d_{2,l+1} \mapsto d_{1,l+1} d_{2l} &> d_{1,l+1} d_{2,l+1}. \end{aligned}$$

This means that our new estimate is at least as good as the old one.

From now on we choose as index for a primitive idempotent $\theta$ the smallest (or sometimes any) value of $s$ satisfying $\theta(\beta^s) \neq 0$. So in this notation, if $\beta^s$ is an $n$th root of unity and $sq^k \equiv s \pmod{n}$, $\theta_s(x)$ is the idempotent of the code with generator $(x^n - 1)/\{(x - \beta^s) \cdot (x - \beta^{sq}) \cdots (x - \beta^{sq^{k-1}})\}$. When applying Theorem 1.5.1, we will always use the optimal ordering of the composing codes, without renumbering explicitly.

Finally, we introduce the Jensen Bound.

**Definition 1.5.2** *The* Jensen Bound *is the estimate for the minimum distance of a cyclic code of length $nN$ found by using Theorem 1.4.4 and Theorem 1.5.1*

An example will not yet be given, for calculations prove to be quite elaborate using only the tools this chapter provides. Moreover not much insight in the structure of 2-D cyclic codes will be gained. Therefore, an example will be postponed until more tools are available (in Chapter 2).

# Chapter 2

# Performance of the Jensen Bound

## 2.1 Shifting

In this section we present the method, called shifting, introduced by Van Lint and Wilson in [6], that yields a lower bound on the minimum distance of a cyclic code. The method only makes use of the zeros of the code. In the next sections we try to apply shifting to 2-D cyclic codes and to compare the results found in this way with those obtained by the Jensen Bound.

We will only give a global idea of how shifting works and introduce the notation we will use in the rest of this chapter. For proofs we refer to [6].

**Definition 2.1.1** *Let $C$ be a cyclic code of length $n$ over $\mathsf{F}_q$, and $\beta$ an $n$th root of unity in an extension field of $\mathsf{F}_q$. The* defining set *$R$ of $C$ is the set of zeros of $C$:*

$$R = \{\beta^r \mid \forall_{\mathbf{c}\in C}[c(\beta^r) = 0]\}.$$

*Furthermore we denote the set of zeros of a codeword $\mathbf{c} \in C$ by $R(\mathbf{c})$.*

Notice that $R = \bigcap_{\mathbf{c}\in C} R(\mathbf{c})$.

**Definition 2.1.2** *If $I = \{i_1, i_2, \ldots, i_l\}$ then the matrix $M(\beta_1, \beta_2, \ldots, \beta_t)_I$ looks as follows:*

$$M(\beta_1, \beta_2, \ldots, \beta_t)_I = \begin{bmatrix} \beta_1^{i_1} & \beta_1^{i_2} & \cdots & \beta_1^{i_l} \\ \beta_2^{i_1} & \beta_2^{i_2} & \cdots & \beta_2^{i_l} \\ \vdots & \vdots & & \vdots \\ \beta_t^{i_1} & \beta_t^{i_2} & \cdots & \beta_t^{i_l} \end{bmatrix}.$$

Let $C$ be a cyclic code with defining set $R$; let $\mathbf{c}$ be a codeword in $C$ with support $I \subseteq \{0, 1, \ldots, n-1\}$; let $c(\beta^l) \neq 0$ and $\{\beta_1, \beta_2, \ldots, \beta_t\} \subseteq R$. Now the following holds (cf. [6]): $\mathrm{r}\left(M\left(\beta_1, \beta_2, \ldots, \beta_t, \beta^l\right)_I\right) = 1 + \mathrm{r}\left(M\left(\beta_1, \beta_2, \ldots, \beta_t\right)_I\right)$, where

$\mathrm{r}(M)$ denotes the rank of the matrix $M$. Moreover, for all $I$ and $\{\beta^{i_1}, \beta^{i_2}, \ldots, \beta^{i_t}\}$ the ranks of $M(\beta^{i_1}, \ldots, \beta^{i_t})_I$ and $M(\beta^{i_1+j}, \ldots, \beta^{i_t+j})_I$ are equal. We can use these two properties to estimate the weight of a codeword. Trivially $\mathrm{wt}(\boldsymbol{c}) \geq \mathrm{r}(M(\beta_1, \beta_2, \ldots, \beta_t)_I)$.

This implies:

$$
\begin{aligned}
\mathrm{wt}(\boldsymbol{c}) &\geq \mathrm{r}(M(\beta_1, \beta_2, \ldots, \beta_t)_I) \\
&= 1 + \mathrm{r}\left(M\left(\beta^{j_1}\beta_1, \beta^{j_1}\beta_2, \ldots, \beta^{j_1}\beta_{t-1}\right)_I\right) \\
&\qquad \text{if } \beta^{j_1}\{\beta_1, \ldots, \beta_{t-1}\} \subseteq R(\boldsymbol{c}) \text{ and } \beta^{j_1}\beta_t \notin R(\boldsymbol{c}) \\
&= 2 + \mathrm{r}\left(M\left(\beta^{j_2}\beta_1, \beta^{j_2}\beta_2, \ldots, \beta^{j_2}\beta_{t-2}\right)_I\right) \\
&\qquad \text{if } \beta^{j_2}\{\beta_1, \ldots, \beta_{t-2}\} \subseteq R(\boldsymbol{c}) \text{ and } \beta^{j_2}\beta_{t-1} \notin R(\boldsymbol{c}) \\
&\vdots \\
&= t - 1 + \mathrm{r}\left(M\left(\beta^{j_{t-1}}\beta_1\right)_I\right) \quad \text{if } \beta^{j_{t-1}}\{\beta_1\} \subseteq R(\boldsymbol{c}) \text{ and } \beta^{j_{t-1}}\beta_2 \notin R(\boldsymbol{c}) \\
&= t \qquad \text{if } \beta^{j_t}\beta_1 \notin R(\boldsymbol{c})
\end{aligned}
$$

In the sequel, this method will be called *shifting*. Clearly, this method does not work for every arbitrary $\{\beta_1, \ldots, \beta_t\}$. We can construct such a set for which the method works 'bottom up' though: start with $\beta_1$ and $\beta^{j_t}$ such that the requirement in the last row is fulfilled; next, find $\beta_2$ and $\beta^{j_{t-1}}$ such that the requirement in the last row but one is fulfilled, and go on like this up to the top row. We capture this idea in the concept of *independent set*.

**Definition 2.1.3** *Let $S \subseteq F$, where $F$ is an extension field of $\mathsf{F}_q$. (In general $S$ will consist of $n$th roots of unity and $F$ will be the smallest extension field of $\mathsf{F}_q$ containing all these roots.) A subset $A$ of $F$ is* independent with respect to $S$ *if it is an element of the family of sets that is constructed inductively as follows:*

1. *$\emptyset$ is independent with respect to $S$;*
2. *If $A$ is independent with respect to $S$, $A \subseteq S$ and $b \notin S$, then $A \cup \{b\}$ is independent with respect to $S$;*
3. *If $A$ is independent with respect to $S$ and $c \in F \backslash \{0\}$, then $cA$ is independent with respect to $S$.*

*Elements $b$ as in 2. will be called* added elements.

This leads us to the following theorem:

**Theorem 2.1.4** *[6] Let $\boldsymbol{c}$ be a word in $(\mathsf{F}_q)^n$; let $F$ be the extension field of $\mathsf{F}_q$ that contains all $n$th roots of unity. Then $\mathrm{wt}(\boldsymbol{c}) \geq |A|$ for all $A \subseteq F$ that are independent with respect to $R(\boldsymbol{c})$.*

The best estimate shifting provides for the minimum distance of a code is called *shifting bound.* For a proof and a somewhat less restricted formulation we refer to [6].

We can determine an independent set using 1, 2 and 3 from Definition 2.1.3:

$$\begin{array}{rcll} A_0 & = & \emptyset & \\ A_1 & = & b_1, & b_1 \notin R(\boldsymbol{c}) \\ A_2 & = & a_2 A_1 \cup \{b_2\}, & b_2 \notin R(\boldsymbol{c}), a_2 A_1 \subseteq R(\boldsymbol{c}) \\ & \vdots & & \\ A_{t-1} & = & a_{t-1} A_{t-2} \cup \{b_{t-1}\}, & b_{t-1} \notin R(\boldsymbol{c}), a_{t-1} A_{t-2} \subseteq R(\boldsymbol{c}) \\ A_t & = & a_t A_{t-1} \cup \{b_t\}, & b_t \notin R(\boldsymbol{c}), a_t A_{t-1} \subseteq R(\boldsymbol{c}) \end{array}$$

To illustrate the ideas in this section we give an example.

**Example 2.1.1** Let $C$ be the binary cyclic code of length 63 with generator $m_0 m_1 m_5 m_{21}$, where $m_i$ denotes the minimal polynomial of $\alpha^i$. Let $\boldsymbol{c}$ be a codeword. Here $R = \{\alpha^i \mid i = 0, 1, 2, 4, 5, 8, 10, 16, 17, 20, 21, 32, 34, 40, 42\}$. We distinguish two cases.

- $c(\alpha^3) = 0$. Now $\boldsymbol{c}$ has 7 consecutive zeros (viz. $\alpha^0, \alpha^1, \ldots, \alpha^6$), so $\mathrm{wt}(\boldsymbol{c}) \geq 8$ by the BCH-bound. (This trivially can be achieved by shifting.)
- $c(\alpha^3) \neq 0$. This implies we can use $\alpha^3$, $\alpha^6$,$\alpha^{12}$, $\alpha^{24}$, $\alpha^{48}$ and $\alpha^{33}$ as added elements. Again we distinguish two cases.
  - $c(\alpha^9) \neq 0$. Sinnce we may use $\alpha^9$ as added element we can shift: $A_0 = \emptyset$, $A_1 = \{\alpha^6\}$, $A_2 = \alpha^{-1} A_1 \cup \{\alpha^6\} = \{\alpha^5, \alpha^6\}$, $A_3 = \alpha^{15} A_2 \cup \{\alpha^{24}\} = \{\alpha^{20}, \alpha^{21}, \alpha^{24}\}$, $A_4 = \alpha^{-16} A_3 \cup \{\alpha^9\} = \{\alpha^4, \alpha^5, \alpha^8, \alpha^9\}$, $A_5 = \alpha^{12} A_4 \cup \{\alpha^{18}\} = \{\alpha^{16}, \alpha^{17}, \alpha^{18}, \alpha^{20}, \alpha^{21}\}$ and $A_6 = \alpha^{-16} A_5 \cup \{\alpha^3\} = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5\}$. We conclude $\mathrm{wt}(\boldsymbol{c}) \geq 6$. We abbreviate the notation of this sequence of independent sets as follows: ($\underline{6}$) $\rightarrow$ (5, $\underline{6}$) $\rightarrow$ (20, 21, $\underline{24}$) $\rightarrow$ (4, 5, 8, $\underline{9}$) $\rightarrow$ (16, 17, $\underline{18}$, 20, 21) $\rightarrow$ (0, 1, 2, $\underline{3}$, 4, 5), where the added elements are underlined.
  - $c(\alpha^9) = 0$. Here $R(\boldsymbol{c})$ contains $R$ and the set$\{\alpha^i \mid i = 9, 18, 36\}$, so we find (in abbreviated notation): ($\underline{3}$) $\rightarrow$ ($2, \underline{3}$) $\rightarrow$ ($1, 2, \underline{3}$) $\rightarrow$ ($16, 17, 18, \underline{24}$) $\rightarrow$ ($8, 9, 10, 16, \underline{24}$) $\rightarrow$ ($0, 1, 2, 8, 16, \underline{24}$); again yielding $\mathrm{wt}(\boldsymbol{c}) \geq 6$.

    Remark: we obtain the same result by the Hartmann-Tzeng bound: $\{1, \alpha, \alpha^2\} \cdot \{1, \alpha^8, \alpha^{16}\} \subset R$.

Since the exact minimum distance of $C$ *is* 6 (see [9, 13]), the shifting bound is sharp for this code.

## 2.2 Zeros of 2-D cyclic codes

In the preceding chapter we have seen that every 2-D cyclic code with $\gcd(n, N) = 1$ is equivalent to a cyclic code of length $nN$. Since this cyclic code is fully identified by its zeros, the corresponding 2-D cyclic code is fully identified by those zeros too. In this section we will see that the zeros of the cyclic code correspond to the zeros of the 2-D cyclic code (in the obvious way). Hence a 2-D cyclic code with $\gcd(n, N) = 1$ is identified by its zeros. We will assume $\gcd(n, N) = 1$ in the rest of this chapter.

Let $\mathcal{C}$ be a 2-D cyclic code over $\mathbb{F}_q$ and let $\alpha$ be a primitive $nN$th root of unity in an extension field of $\mathbb{F}_q$.

The zeros of $\mathcal{C}$ (regarded as a cyclic code, where (as before) we take $Z = xy$) are powers of $\alpha$, say $\alpha^{l_k}$, $k = 1, 2, \ldots, t$. That is: $\sum_{\mu=0}^{nN-1} c_\mu (\alpha^{l_k})^\mu = 0$ for all $k \in \{1, 2, \ldots, t\}$ and all codewords $\boldsymbol{c}$ in $\mathcal{C}$.

The Euclidian Algorithm provides $\lambda$ and $\mu$ such that $\lambda N + \mu n = 1$. Now $\beta = \alpha^{\lambda N}$ is a primitive $n$th root of unity, and $\gamma = \alpha^{\mu n}$ a primitive $N$th root of unity, and $\alpha = \beta\gamma$. Thus a power of $\alpha$ can be written as a product of powers of $\beta$ and $\gamma$: $\alpha^l = \beta^l \gamma^l = \beta^{l \bmod n} \gamma^{l \bmod N}$.

Notice that a coefficient $c_\nu$ in the cyclic code corresponds to the coefficient $c_{\nu \bmod n, \nu \bmod N}$ in the 2-D cyclic code. From this it follows that if $Z = \alpha^l$ is a zero of a word $\boldsymbol{c} \in \mathcal{C}$ (as a cyclic code), then $(x, y) = (\beta^{l \bmod n}, \gamma^{l \bmod N})$ is a zero of $\boldsymbol{c}$ considered as a word in the 2-D cyclic code:

$$\begin{aligned} \sum_{\nu=0}^{nN-1} c_\nu \alpha^{l\nu} &= \sum_{\nu=0}^{nN-1} c_\nu \beta^{l\nu} \gamma^{l\nu} \\ &= \sum_{\nu=0}^{nN-1} c_{\nu \bmod n, \nu \bmod N} \beta^{l\nu \bmod n} \gamma^{l\nu \bmod N} \\ &= \sum_{i=0}^{n-1} \sum_{j=0}^{N-1} c_{ij} (\beta^{l \bmod n})^i (\gamma^{l \bmod N})^j. \end{aligned} \tag{2.1}$$

This enables us to find the zeros of a 2-D cyclic code from the zeros of the corresponding cyclic code, and vice versa. A similar relationship between the (non)zeros of the inner and outer codes and the (non)zeros of the concatenation of those codes will prove to be very useful in almost any calculation involving a 2-D cyclic code. Especially these results, and the way in which they are derived, will be crucial in the proof of Theorem 2.3.2.

First we investigate the case $\mathcal{C} = \langle \theta_s \rangle \Box \mathcal{B}$. The nonzeros of $\langle \theta_s \rangle$ are the elements of the cyclotomic coset mod$n$ containing $\beta^s$; let it have cardinality $k$ (i.e., $\beta^{sq^k} = \beta^s$). Let the nonzeros of the outer code $\mathcal{B}$ be $\gamma_1, \gamma_2, \ldots, \gamma_K$. Now, for any codeword $\boldsymbol{c}$,

$$c(\beta^{sq^i}, \gamma_j^{q^i}) = \sum_{u=0}^{n-1} \sum_{v=0}^{N-1} c_{uv} \beta^{sq^i u} \gamma_j^{q^i v} = \sum_{v=0}^{N-1} \gamma_j^{q^i v} \sum_{u=0}^{n-1} c_{uv} (\beta^{sq^i})^u, \tag{2.2}$$

where the inner sum represents a word in $\mathbb{F}_q G_x$ for all $v$; therefore it equals $\{\sum_{u=0}^{n-1} c_{uv}(\beta^s)^u\}^{q^i}$. This in turn —assuming (w.l.o.g.) that $\beta^s$ is the value chosen for $\beta_s$ in the definition of $\phi_s$— equals $(\phi_s(c_v))^{q^i}$, where $c_v$ is the polynomial $\sum_{u=0}^{n-1} c_{uv}x^u$. Hence

$$c(\beta^{sq^i}, \gamma_j^{q^i}) = \sum_{v=0}^{N-1} (\phi_s(c_v)\gamma_j^v)^{q^i} = \left(\sum_{v=0}^{N-1} \phi_s(c_v)\gamma_j^v\right)^{q^i} \neq 0,$$

for the vector $(\phi_s(c_1), \phi_s(c_2), \ldots, \phi_s(c_{N-1}))$ exactly equals the word in $\mathcal{B}$ corresponding to the word in $\mathcal{C}$ we started with, and $\gamma_j$ is a nonzero of $\mathcal{B}$. Hence all the pairs $(\beta^{sq^i}, \gamma_j^{q^i})$, $0 \leq i < k$, $1 \leq j \leq K$ are nonzeros of $\mathcal{C}$. All those pairs are different, so we have found $kK$ nonzeros. Since $\dim \mathcal{C} = kK$ these are *all* the nonzeros of $\mathcal{C}$. So we have proved the following lemma.

**Lemma 2.2.1** *[8] Let $\langle\theta_s\rangle$ have nonzeros $\beta^{sq^i}$, $0 \leq i < k$ and let $\mathcal{B}$ have nonzeros $\gamma_1, \gamma_2, \ldots, \gamma_K$. Then, assuming that $\phi_s(a) = a(\beta^s)$ for $a \in \langle\theta_s\rangle$, $\langle\theta_s\rangle \square \mathcal{B}$ has nonzeros $(\beta^{sq^i}, \gamma_j^{q^i})$, $0 \leq i < k$ and $1 \leq j \leq K$.*

The set of nonzeros of a 2-D cyclic code $\mathcal{C} = \bigoplus_{s=1}^{v} \mathcal{C}_s$ can be found by taking the union of the sets of nonzeros of the $\mathcal{C}_s$.

The following corollary is used in the derivation of Lemma 2.3.1 and Theorem 2.3.2.

**Corollary 2.2.2** *A pair $(\beta, \gamma)$ of an $n$th and an $N$th root of unity is a nonzero of the 2-D cyclic code $\langle\theta_s\rangle \square \mathcal{B}$ if and only if $\beta = \beta_s^{q^i}$ and $\gamma = \gamma_j^{q^i}$, where $\beta_s$ is the nonzero of $\theta_s$ that is used in the definition of $\phi_s$, and $\gamma_j$ is a nonzero of $\mathcal{B}$.*

When calculating the Jensen Bound for a cyclic code, one might expect that the next four choices influence the value one finds in Equation 1.1.

1. The choice of $G_x$ and $G_y$ given $G$ (i.e., the choice of $n$ and $N$ given $nN$).

2. The relationship between the generators $Z$ of $G$ on the one hand, and $x$ and $y$ of $G_x$ and $G_y$ on the other hand.

   The natural choice of course is $Z = xy$, but any choice $Z = x^a y^b$ with $\gcd(a, n) = \gcd(b, N) = 1$ is legitimate. If $a$ and $b$ are not both equal to 1, a codeword is put in matrix form in a different way compared to the case $Z = xy$. Hence the inner and outer codes may change. It is not at first sight clear if the the right hand side in Equation 1.1 remains the same. In Example 2.2.1 we will see it does.

3. The relationship between the $nN$th root of unity $\alpha$ and the $n$th and $N$th roots of unity $\beta$ and $\gamma$.

The natural choice would, if $Z = xy$, be to take $\beta$ and $\gamma$ such that $\alpha = \beta\gamma$, for in that case a (non)zero $\alpha^l$ corresponds to a (non)zero $(\beta^{l \bmod n}, \gamma^{l \bmod N})$. But again any choice $\alpha = \beta^a\gamma^b$ with $\gcd(a,n) = \gcd(b,N) = 1$ is legitimate, and again inner and outer codes may differ to those found using the natural choice. (And again the estimate of $d$ remains the same; see Example 2.2.1 below.)

4. The choice of $\beta_s$ given a minimal cyclic code $\langle\theta_s\rangle$.

   Obviously this choice determines the maps $\phi_s$ and $\Phi_s$ (and their inverses). In Example 2.2.1 however, we will see that the estimate of $d$ does not depend on it.

**Example 2.2.1** Let $C$ be the binary cyclic code of length 63 with check polynomial $m_1(Z)m_{11}(Z)$. $C$ has nonzeros $\alpha^i$, $i = 1, 2, 4, 8, 11, 16, 22, 25, 32, 37, 44, 50$.

A) $n = 7$, $N = 9$, $\beta = \alpha^{36}$, $\gamma = \alpha^{28}$. (This is the choice of $\beta$ and $\gamma$ as in the beginning of this section, and indeed $\alpha = \beta\gamma$.)

As a 2-D cyclic code the zeros of $C$ are: $(\beta^i, \gamma^j)$, $(i,j) = (1,1), (2,2), (4,4), (1,8), (2,7), (4,5), (4,2), (1,4), (2,8), (4,7), (1,5), (2,1)$ (corresponding to $\alpha^i$, $i = 1,2,4,8,16,32,11,22,44,25,50,37$ respectively). It is easy to see that the (only) inner code is $\langle\theta_1\rangle$, with nonzeros $\beta$, $\beta^2$ and $\beta^4$. $\langle\theta_1\rangle$ has minimum distance 4.

1. If we take $\beta_s = \beta$, we find as nonzeros of the outer code $\mathcal{B}$: $\gamma, \gamma^8, \gamma^4, \gamma^5$, i.e., $\mathcal{B} = M_1^- \oplus M_4^-$.[1] Then $\mathcal{B}$ has minimum distance 5.
2. If we take $\beta_s = \beta^2$, the nonzeros of $\mathcal{B}$ are $\gamma^2, \gamma^7, \gamma^8, \gamma^1$, so $\mathcal{B} = M_1^- \oplus M_2^-$, with minimum distance 5.
3. For $\beta_s = \beta^4$ we find $\mathcal{B} = M_2^- \oplus M_4^-$, again with minimum distance 5.

Conclusion: Theorem 1.5.1 yields $d \geq 20$ in all three cases.
This is not so just by accident: notice that a change of $\beta_s = \beta^i$ to $\beta_s = \beta^{iq}$ results in a new outer code $\mathcal{B}$ that can be found from the old one by the map $\gamma \to \gamma^q$ (for its zeros can be found this way). This means that for any word $\sum b_j y^j$ in the old code we can find one (unique) word $\sum b_j^q y^j$ (of course with the same support) in the new one. Hence both codes have the same minimum distance. The inner code of course does not change at all, so neither does the related estimate for $d$.

[1] Outer codes will be denoted as a direct sum of minimal cyclic codes; throughout this paper these minimal cyclic codes are denoted $M_i^-$, where $\gamma^i$ is a nonzero of the idempotent of this code. Notice that the field in which the letters of the code lie must follow from the context (i.e., from the dimension of the corresponding inner code). In a sum $\langle\theta_0\rangle \square M_1^- \oplus \langle\theta_1\rangle \square M_1^-$ the first $M_1^-$ is a $q$-ary code; the second $M_1^-$ is a code over $\mathbb{F}_{q^k}$; $k$ need not be equal to 1!

B) $Z = x^3y$, the rest as above. In this case a coefficient $c_\mu$ in the cyclic code corresponds to $c_{3\mu \bmod n, \mu \bmod N}$ in the 2-D cyclic code. Analogous to the discussion at the beginning of this section we find: $Z = \alpha^l$ is a zero if and only if $(x, y) = (\beta^{1/3 \cdot l \bmod n}, \gamma^{l \bmod N})$ is a zero.

So in this case the nonzeros of $C$ are:$(\beta^i, \gamma^j)$, $(i, j) = (5,1)$, $(3,2)$, $(6,4)$, $(5,8)$, $(3,7)$, $(6,5)$, $(5,4)$, $(3,8)$, $(6,7)$, $(5,5)$, $(3,1)$, $(4,2)$. ($5 = 1/3 \cdot 1 \bmod 7$, $3 = 1/3 \cdot 2 \bmod 7$, etc.). So the inner code is $\langle \theta_3 \rangle$ with minimum distance 4, and $\beta_s = \beta^3$ yields $\mathcal{B} = M_1^- \oplus M_2^-$ with minimum distance 5. Hence $d \geq 20$.

C) $Z = xy^5$, the rest as above. In this case $Z = \alpha^l$ is a zero if and only if $(x, y) = (\beta^{l \bmod n}, \gamma^{1/5 \cdot l \bmod N})$ is a zero. With this it follows that $C = \langle \theta_1 \rangle \square (M_1^- \oplus M_2^-)$, again yielding $d \geq 5 \cdot 4 = 20$.

From B) and C) we see that $Z = x^3y$ changes the inner code only (compared to the code yielded by $Z = xy$), and $Z = xy^5$ changes the outer code only. In fact it is not hard to prove that in general $Z = x^a y^b$ results in inner codes $\langle \theta_i \rangle$, where $\beta^{ia}$ is a zero of an inner code $\langle \theta_{ia} \rangle$ we find using $Z = xy$. For the outer codes $\mathcal{B}_i$, any zero $\gamma_j$ corresponds to a zero $\gamma_j^b$ of an outer code we find using $Z = xy$. This means that neither of the minimum distances is different from those found by using $Z = xy$. (Any cyclic code maps into an equivalent code under the map $\xi \mapsto \xi^a$ (where $\xi$ is the primitive root used in the code, and $a$ is coprime with the length of the code), for any old word $\sum b_i y^i$ corresponds to a (unique) new word $\sum b_{ia} y^i$ (for obviously $\sum b_{ia} y^i$ has a zero $\zeta^a$ if and only if $\sum b_i y^i$ has a zero $\zeta$).)

D) $Z = xy$, $\beta = \alpha^9$, $\gamma = \alpha^7$ (i.e., $\alpha = \beta^4 \gamma^4$). Here $Z = \alpha^l$ is a zero if and only if $(x, y) = (\beta^{4l \bmod n}, \gamma^{4l \bmod N})$ is a zero (use Equation 2.1). Analogous to the calculations above, we find $C = \langle \theta_1 \rangle \square (M_1^- \oplus M_2^-)$ (with $\beta_s = \beta^4$); and again Equation 1.1 yields $d \geq 20$.

In general any legitimate choice of $\beta$ and $\gamma$ will yield $\alpha = \beta^a \gamma^b$ for some $a$ and $b$ with $\gcd(a, n) = \gcd(b, N) = 1$, which in turn results in the 'equivalence' of $\alpha^l$ and $(\beta^{al \bmod n}, \gamma^{bl \bmod N})$. Analogous to the discussion immediately above D) we find that any legitimate choice of $\beta$ and $\gamma$ gives inner and outer codes equivalent to those found with the natural choice (s.t. $\alpha = \beta\gamma$), and thus yields the same value in Equation 1.1.

From now on it is always (unless indicated otherwise) assumed that $Z = xy$, $\alpha = \beta\gamma$ and all $\beta_s$ are those nonzeros of the $\langle \theta_s \rangle$ that are the smallest power of $\beta$.

Finally we come to the choice of $n$ and $N$, given their product. This choice *does* influence the value in Equation 1.1.

E) $n = 9$, $N = 7$. Of course we find the zeros of A), only the order of the $n$th and $N$th roots of unity is reversed: $(\beta^i, \gamma^j)$ under A) is denoted $(\beta^j, \gamma^i)$ here.

Then $C = \langle\theta_1\rangle\Box(M_1^- \oplus M_2^-)$, (the $M_i^-$ are codes over $\mathbf{F}_{64}$ having only one nonzero ($\mathbf{F}_{64}$ contains all 7th roots of unity!)). Equation 1.1 yields $d \geq 2 \cdot 6 = 12$.

Conclusion: The choice of $x$, $y$, $\beta$, $\gamma$ and of the $\beta_s$ does not influence the value Equation 1.1 yields; the choice of $n$ and $N$ does.

## 2.3 2-D cyclic codes and Shifting

### 2.3.1 Introduction

In Subsection 2.3.2 we attempt to make a comparison of the performances of the Jensen Bound and shifting. To do this, shifting is applied to a cyclic code, making use of its structure as a 2-D cyclic code; more precisely: of independent sets with respect to the zeros of the inner and outer codes. This yields an equation much like Equation 1.1, and in fact some extra requirements on the inner and outer codes guarantee that shifting provides at least as good an estimate on the minimum distance as the Jensen Bound does. All binary cyclic codes of length 63 fulfill these requirements on their inner and outer codes (Subsection 2.3.3).

### 2.3.2 Independent sets and 2-D cyclic codes

To be able to compare shifting to the Jensen Bound, one must

either obtain (an estimate of) the Jensen Bound from the knowledge of the zeros of a word of minimum weight (or even from an independent set with respect to those zeros)

or produce an independent set (with respect to the set of zeros of a word of minimum weight) from the knowledge of the 2-D cyclic code (especially the inner and outer codes).

The latter is tried in this subsection.

Let $C = \bigoplus_{s=1}^{v} C_s$, $C_s = \langle\theta_s\rangle\Box\mathcal{B}_s$, $s = 1, 2, \ldots, v$ and $\boldsymbol{c} = \sum_{s=1}^{v} \boldsymbol{c}_s$, $\boldsymbol{c}_s \in C_s$ for all $s$. Every component $\boldsymbol{c}_s$ of $\boldsymbol{c}$ is the image under $\Psi_s$ of a word in $\mathcal{B}_s$: $\boldsymbol{c}_s = \Psi_s(\boldsymbol{b}_s)$, $\boldsymbol{b}_s \in \mathcal{B}_s$. Denote the $i$th column of $\boldsymbol{c}_s$ as $\boldsymbol{c}_{si}$ or (as a polynomial) as $c_{si}$.

Let, for all values[2], of $s$, $B_1^{(s)} = \{\gamma_{s1}\}$, $B_2^{(s)} = b_{s2}B_1^{(s)}, \cup\{\gamma_{s2}\}, \ldots, B_{d_{2s}}^{(s)} = b_{s,d_{2s}}B_{d_{2s}-1}^{(s)} \cup \{\gamma_{s,d_{2s}}\}$ be a sequence of independent sets with respect to $R(\boldsymbol{b}_s)$, and $A_1^{(s)} = \{\beta_{s1}\}$, $A_2^{(s)} = a_{s2}A_1^{(s)} \cup \{\beta_{s2}\}, \ldots, A_{d_{1s}}^{(s)} = a_{s,d_{1s}}A_{d_{1s}-1}^{(s)} \cup \{\beta_{s,d_{1s}}\}$ a sequence of independent sets with respect to $R(\theta_1 + \theta_2 + \cdots + \theta_s)$, where all $\beta_{si}$ are nonzeros of $\theta_s$. Write $\beta_{si} = \beta_s^{t_i}$, where of course each $t_i$ is a power of $q$.

[2] we will choose one specific value in Lemma 2.3.1 and use all of them in Theorem 2.3.2

**Lemma 2.3.1** *If* $s = \max\{t \mid \exists_i[c_{ti}(\beta_t) \neq 0]\}$ *(where* $\beta_t$ *is a nonzero of* $\theta_t$*), in other words: if* $\boldsymbol{b} = \boldsymbol{b}_1 + \cdots + \boldsymbol{b}_s$, $\boldsymbol{b}_s \neq \boldsymbol{0}$ *and* $\boldsymbol{b}_t = \boldsymbol{0}$ *for* $t > s$*, then the set* $C^{(s)}_{d_{1s},d_{2s}}$ *constructed below is independent with respect to* $R(\boldsymbol{c})$.

$$
\begin{aligned}
C^{(s)}_{11} &= \{\beta_{s1}\gamma_{s1}^{t_1}\} \qquad (2.3)\\
C^{(s)}_{12} &= b_{s2}^{t_1} C^{(s)}_{11} \cup \{\beta_{s1}\gamma_{s2}^{t_1}\}\\
&\vdots\\
C^{(s)}_{1d_{2s}} &= b_{s,d_{2s}}^{t_1} C^{(s)}_{1,d_{2s}-1} \cup \{\beta_{s1}\gamma_{s,d_{2s}}^{t_1}\}\\
C^{(s)}_{21} &= a_{s2} C^{(s)}_{1d_{2s}} \cup \{\beta_{s2}\gamma_{s1}^{t_2}\}\\
C^{(s)}_{22} &= b_{s2}^{t_2} C^{(s)}_{21} \cup \{\beta_{s2}\gamma_{s2}^{t_2}\}\\
&\vdots\\
C^{(s)}_{2d_{2s}} &= b_{s,d_{2s}}^{t_2} C^{(s)}_{2,d_{2s}-1} \cup \{\beta_{s2}\gamma_{s,d_{2s}}^{t_2}\}\\
&\vdots\\
C^{(s)}_{d_{1s},1} &= a_{s,d_{1s}} C^{(s)}_{d_{1s}-1,d_{2s}} \cup \{\beta_{s,d_{1s}}\gamma_{s1}^{t_{d_{1s}}}\}\\
C^{(s)}_{d_{1s},2} &= b_{s2}^{t_{d_{1s}}} C^{(s)}_{d_{1s},1} \cup \{\beta_{s,d_{1s}}\gamma_{s2}^{t_{d_{1s}}}\}\\
&\vdots\\
C^{(s)}_{d_{1s},d_{2s}} &= b_{s,d_{2s}}^{t_{d_{1s}}} C^{(s)}_{d_{1s},d_{2s}-1} \cup \{\beta_{s,d_{1s}}\gamma_{s,d_{2s}}^{t_{d_{1s}}}\}
\end{aligned}
$$

*This can be summarized in: Equation 2.3,*

$$C^{(s)}_{i,j+1} = b_{s,j+1}^{t_i} C^{(s)}_{ij} \cup \{\beta_{si}\gamma_{s,j+1}^{t_i}\}, \quad 1 \leq i \leq d_{1s}, 1 \leq j < d_{2s} \qquad (2.4)$$

$$C^{(s)}_{i+1,1} = a_{s,i+1} C^{(s)}_{i,d_{2s}} \cup \{\beta_{s,i+1}\gamma_{s1}^{t_{i+1}}\}, \quad 1 \leq i < d_{1s} \qquad (2.5)$$

Remark: Notice that the construction falls apart into $d_{1s}$ parts, each consisting of $d_{2s}$ steps. Each part applies the construction of $B^{(s)}_{d_{2s}}$ in a 'twisted' way. The way in which it is twisted in the $i$th part is decided by $a_{si}$ and $\beta_{si}$ (from the construction of $A^{(s)}_{d_{1s}}$). The whole construction roughly is a product of the constructions of $A^{(s)}_{d_{1s}}$ and $B^{(s)}_{d_{2s}}$, in fact $C^{(s)}_{1i} = A^{(s)}_1 (B^{(s)}_i)^{t_i}$.

**Proof:** It is sufficient to prove that:

1. all added elements $\beta_{si}\gamma_{sj}^{t_i}$ are nonzeros of $\boldsymbol{c}$;
2. all sets $a_{si} C^{(s)}_{i,d_{2s}}$ and $b_{sj}^{t_i} C^{(s)}_{i,j-1}$ are subsets of $R(\boldsymbol{c})$ (i.e., contain only zeros of $\boldsymbol{c}$).

Proof of 1: $\beta_{si}$ is a nonzero of $\theta_s$; $\gamma_{sj}$ is a nonzero of $\boldsymbol{b}_s$. Hence $c_s(\beta_{si}, \gamma_{sj}^{t_i}) = c(\beta_s^{t_i}, \gamma^{t_i}) \neq 0$, because $t_i$ is a power of $q$. (Use Corollary 2.2.2.)

Since $\beta_{si}$ is a zero of all $\langle\theta_t\rangle$, $t \neq s$, the pair $(\beta_{si}, \gamma_{sj}^{t_i})$ is a zero of all $\boldsymbol{c}_t$, $t \neq s$. (Again as a consequence of Corollary 2.2.2.) Hence $c(\beta_{si}, \gamma_{sj}^{t_i}) = c_s(\beta_{si}, \gamma_{sj}^{t_i}) \neq 0$.

Proof of 2.: To prove this, all sets $C_{ij}^{(s)}$ are split into two halves:

the inheritance of the previous part: $C_{i-1,d_{2s}}^{(s)}$ multiplied by $a_{si}b_{s2}^{t_i}b_{s3}^{t_i}\cdots b_{sj}^{t_i}$;

the elements introduced in the current part: multiplied by a factor as well: $\beta_{si}\gamma_{sl}^{t_i}$ is multiplied by $b_{s,l+1}^{t_i}b_{s,l+2}^{t_i}\cdots b_{sj}^{t_i}$, $(1 \le l < j)$.

Any $nN$th root of unity can be written in a unique way as the product of an $n$th and an $N$th root of unity. Those factors are called the $\beta$-component respectively the $\gamma$-component. It is easy to prove by induction that the $\beta$-components of the elements of any $C_{i,d_{2s}}^{(s)}$ are in $A_i^{(s)}$. Thus the inheritance of the previous part has as $\beta$-component the product of an element of $A_{i-1}^{(s)}$ and $a_{si}$, so its $\beta$-component is a zero of $\theta_1 + \theta_2 + \cdots + \theta_s$, i.e., it is a zero of all $\theta_i$, $1 \le i \le s$, and thus all elements of the inheritance are zeros. (Use Corollary 2.2.2 again.)

The newly introduced elements have $\gamma$-component $\gamma_{sl}^{t_i}b_{s,l+1}^{t_i}b_{s,l+2}^{t_i}\cdots b_{sj}^{t_i}$, which is an element (and *not* the added element) of $B_j^{(s)}$ to the power $t_i$. So the $\gamma$-components are zeros of $\boldsymbol{b}_s$ to the power $t_i$. This implies that the elements themselves can*not* be of the form $(\beta_s^{q^t}, \gamma_j^{q^t})$ with $\gamma_j$ a nonzero of $\boldsymbol{b}_s$, so they must be zeros of the concatenation of $\langle\theta_s\rangle$ and any code containing $\boldsymbol{b}_s$, and thus of $\boldsymbol{c}_s$ as well. Since $\beta_{si}$ trivially is a zero of all $\langle\theta_t\rangle$, $(t \ne s)$, $\beta_{si}\gamma_{sl}^{t_i}b_{s,l+1}^{t_i}\cdots b_{sj}^{t_i}$ is a zero of all other $\boldsymbol{c}_t$, $t \ne s$, as well, and hence a zero of $\boldsymbol{c}$. □

This lemma, together with Theorem 2.1.4 provides the tools necessary to apply shifting to a 2-D cyclic code. The words of such a code $C$ can be partitioned into $v+1$ classes corresponding to the value of $s$ in the lemma: $v$ classes corresponding to the $v$ possible values of $s$, and one extra class containing those words for which no $t$ exists such that $\exists_i[c_{ti}(\beta_t) \ne 0]$.

This last class thus consists of all $\boldsymbol{c} = \sum \boldsymbol{c}_t$ where all columns $c_{ti}$ have a zero $\beta_t$. Since this is the 'only' nonzero of $\langle\theta_t\rangle$ (which is the code that contains all $c_{ti}$), all $c_{ti}$ must be equal to the zero word (being the only word that is zero in all $n$th roots of unity), so $\boldsymbol{c} = \boldsymbol{0}$.

All other classes contain nonzero words only, and allow application of the lemma above and Theorem 2.1.4. Given a class, the value found this way is decided by the zeros of the $\boldsymbol{b}_s$ only. Hence this value depends only on the shifting bound for the $\mathcal{B}_s$. This proves the next theorem.

**Theorem 2.3.2** *If, for $1 \le s \le v$, $d_{1s}$ is the cardinality of the largest independent set with respect to $R(\theta_1 + \theta_2 + \cdots + \theta_s)$ with the extra assumption that all added elements are nonzeros of $\theta_s$, and if $d_{2s}$ is the shifting bound for the $\mathcal{B}_s$, then the shifting bound $d_{\text{shift}}$ for $C = \bigoplus_{s=1}^{v}\langle\theta_s\rangle\square\mathcal{B}_s$ satisfies:*

$$d_{\text{shift}} \ge \min\{d_{1s}d_{2s} \mid 1 \le s \le v\}. \tag{2.6}$$

This theorem does not allow a general comparison of the Jensen Bound and shifting, but it will help to make this comparison for specific codes, and will give some insight in the performance of both bounds in general, as we will see in the next subsection.

First however, we will investigate the situation that arises when the extra assumption in Theorem 2.3.2 is *not* made. In that case there may be $\beta_{si}$ that are nonzeros of some other $\theta_l$, $1 \leq l < s$. Then write $\beta_{si} = \beta_l^{t_i}$ (where $t_i$ is a power of $q$). Now $\beta_l^{t_i}\gamma_{sj}^{u_i}$ is a nonzero of $\boldsymbol{c}$ if and only if $\gamma_{sj}^{u_i}$ equals a nonzero of $\mathcal{B}_l$ to the power $t_i$ (for $\beta_l^{t_i}\gamma_{sj}^{t_i}$ is a zero of all $\boldsymbol{c}_t$ with $t \neq l$). This is the case if $\gamma_{sj}$ itself is a nonzero of $\mathcal{B}_l$ and $u_i = t_i$.

As soon as this assumption on the $\gamma_{sj}$ is made, all the arguments under 'Proof of 1' become valid again if we let $\theta_l$ play the role of $\theta_s$. Since the arguments concerning the inherited elements are not affected at all, we even can replace the $B_j^{(s)}$, $(1 \leq j \leq d_{2s})$, by $B_j^{(l)}$, $(1 \leq j \leq d_{2l})$. If we do this, the arguments concerning the newly added elements become valid as well. This proves the next lemma.

**Lemma 2.3.3** *If $s$ is defined as in Lemma 2.3.1; if the $A_i^{(s)}$ and $B_i^{(l)}$ constitute sequences of independent sets with respect to $R(\theta_1 + \theta_2 + \cdots + \theta_s)$ for all (appropriate) $i$ and all $l$, $1 \leq l \leq s$; and if we denote $\beta_{si} = \beta_{l_i}^{t_i}$, then the sets constructed as follows*

$$\begin{aligned} C_{11}^{(s)} &= \{\beta_{s1}\gamma_{l_1,1}^{t_1}\}; \\ C_{i,j+1}^{(s)} &= b_{l_i,j+1}^{t_i} C_{ij}^{(s)} \cup \{\beta_{si}\gamma_{l_i,j+1}^{t_i}\}, 1 \leq i \leq d_{1s},\ 1 \leq j < d_{2,l_i}; \\ C_{i+1,1}^{(s)} &= a_{s,i+1} C_{i,d_{2l_i}}^{(s)} \cup \{\beta_{s,i+1}\gamma_{l_{i+1},1}^{t_i}\},\ 1 \leq i < d_{2s}; \end{aligned}$$

*are independent with respect to $R(\boldsymbol{c})$.*

This allows the conclusion that

$$\mathrm{wt}(\boldsymbol{c}) \geq \sum_{i=1}^{d_{1s}} d_{2l_i}.$$

Therefore we can drop the extra assumptions on the $A_i^{(s)}$ in Theorem 2.3.2 without consequence for the bound this theorem yields, if all the $d_{2l_i}$ are equal to $d_{2s}$.

### 2.3.3 Application to $nN = 63$.

In this subsection the ideas of the previous subsection are applied to all binary cyclic codes of length 63. First, two examples of the construction of independent sets as in Lemma 2.3.1 are given; next, it is examined for all codes if the assumptions on the inner and outer codes from Theorem 2.3.2 are satisfied.

**Example 2.3.1** Let $\mathcal{C}$ be the code of Example 2.1.1. Then $\mathcal{C}$ has nonzeros $\alpha^i$, $i = 3, 6, 7, 9, 11$–$15, 18, 19, 22$–$31, 33, 35$–$39, 41, 43$–$62$. (Here $a$–$b$ denotes the numbers $a$ to $b$ inclusive.)

For $n = 7$, $N = 9$, we find $\mathcal{C}_0 = \langle\theta_0\rangle\Box M_1^-$, corresponding to the zeros of $m_7$; $\mathcal{C}_1 = \langle\theta_1\rangle\Box(M_0^- \oplus M_4^- \oplus M_3^- \oplus M_2^-)$, corresponding to the zeros of $m_9$, $m_{11}$, $m_{15}$ and $m_{23}$ respectively; $\mathcal{C}_3 = \langle\theta_3\rangle\Box(M_3^- \oplus M_2^- \oplus M_0^- \oplus M_4^-)$, corresponding to the zeros of $m_3$, $m_{13}$, $m_{27}$ and $m_{31}$ respectively. Equation 1.1 yields $d \geq \min\{7 \cdot 2, 3 \cdot 3, 1 \cdot 3\} = 3$, for the minimum distances of the outer codes are 2, 3, and 3 respectively.

For $n = 9$, $N = 7$ we find $\mathcal{C}_0 = \langle\theta_0\rangle\Box(M_1^- \oplus M_3^-)$; $\mathcal{C}_1 = \langle\theta_1\rangle\Box(M_0^- \oplus M_2^- \oplus M_5^- \oplus M_4^- \oplus M_6^-)$; $\mathcal{C}_3 = \langle\theta_3\rangle\Box(M_3^- \oplus M_1^-)$; from this it follows that $d \geq \min\{9 \cdot 2, 3 \cdot 2, 1 \cdot 3\} = 3$. (The order of $\mathcal{C}_1$ and $\mathcal{C}_3$ is implicitly reversed here.)

**Conclusion:** The Jensen Bound for $\mathcal{C}$ is 3.

Note that for this code the BCH-bound is 4, so this is an example of poor performance of the Jensen Bound. However, this does not imply that this code is not illustrative for the methods of the previous subsection.

We will now construct independent sets with respect to words of $\mathcal{C}$ as in Theorem 2.3.2. Since the independent sets corresponding to the Jensen Bound use independent sets of cardinality 1 and 3 for the inner respectively outer codes, (as these are the values of $d_{1s}$ and $d_{2s}$ for which the minimum in Equation 1.1 is taken), we take a look at a second one to gain more insight into the construction.

We take $n = 7$, $N = 9$. Of course this choice is of no influence here. First we renumber the $\mathcal{C}_s$ as follows: $\mathcal{C}_0 \mapsto \mathcal{C}_1$; $\mathcal{C}_1 \mapsto \mathcal{C}_2$; $\mathcal{C}_3 \mapsto \mathcal{C}_3$. This will help to keep notation clear.

Since $\theta_1 + \theta_2 + \theta_3 = 1$, an independent set with respect to $R(\theta_1 + \theta_2 + \theta_3)$, with the extra assumption that all added elements are nonzeros of $\theta_3$, is $A_1^{(3)} = \{\beta^3\}$. Moreover this set cannot be extended, as 1 (as a polynomial) has no zeros.

The outer code $\mathcal{B}_3$ has nonzeros 0; $\gamma^2$ and $\gamma^7$; $\gamma^3$ and $\gamma^6$; $\gamma^4$ and $\gamma^5$. If we assume $\gamma^3$ to be a nonzero of a word of minimal weight of $\mathcal{B}_3$, we find, using the sequence of independent sets (w.r.t. this word) $B_1^{(3)} = \{\gamma^3\}$, $B_2^{(3)} = \gamma^7 B_1^{(3)} \cup \{\gamma^3\} = \{\gamma, \gamma^3\}$, $B_3^{(3)} = \gamma^7 B_2^{(3)} \cup \{\gamma^3\} = \{\gamma, \gamma^8, \gamma^3\}$, that the weight of this word is at least 3.

We may indeed assume $\gamma^3$ to be a nonzero, for if it is a zero, assume $\gamma^4$ to be a nonzero and take $\gamma_i = \gamma^4$ and $b_{si} = \gamma^2$ for all $i$; now we find wt $\geq 5$; if both $\gamma^3$ and $\gamma^4$ are zeros, the BCH-bound (which trivially can be achieved by shifting) yields wt $\geq 5$.

This means that the shifting bound for $\mathcal{B}_3$ is 3, and that this sequence of $B_i^{(3)}$ is a sequence that satisfies the conditions of Theorem 2.3.2.

We follow the construction of Lemma 2.3.1. Since $\beta_3 = \beta^3$, all the $t_i$ are equal to 1. So $C_{11}^{(3)} = \{\beta^3\gamma^3\} = \{\alpha^3\}$, $C_{12}^{(3)} = \gamma^7 C_{11}^{(3)} \cup \{\beta^3\gamma^3\} = \{\alpha^{10}, \alpha^3\}$,

$C_{13}^{(3)} = \gamma^7 C_{12}^{(3)} \cup \{\beta^3\gamma^3\} = \{\alpha^{17}, \alpha^{10}, \alpha^3\}$. $C_{13}^{(3)}$ is 'maximal': there is no $c_4$ such that $c_4 C_{13}^{(3)} \subseteq R(\mathcal{C})$.

As a second example, $C_{33}^{(2)}$ is constructed in the same way. We take $A_1^{(2)} = \{\beta\}$, $A_2^{(2)} = \beta A_1^{(2)} \cup \{\beta^4\} = \{\beta^3, \beta^4\}$, $A_3^{(2)} = \beta^2 A_2^{(2)} \cup \{\beta\} = \{\beta^5, \beta^6, \beta\}$ as independent sets with respect to $R(\theta_1 + \theta_2)$. ($\theta_1 + \theta_2$ has nonzeros $\beta$, $\beta^2$, $\beta^4$, and 1.) Note that all added elements are nonzeros of $\theta_2$.

$\mathcal{B}_2$ is the same code as $\mathcal{B}_3$; since the structure of the construction probably will become clearer if the $b$'s and $\gamma$'s are different, we take $B_1^{(2)} = \{\gamma^3\}$, $B_2^{(2)} = \gamma^5 B_1^{(2)} \cup \{\gamma^6\} = \{\gamma^8, \gamma^6\}$, $B_3^{(2)} = \gamma^2 B_2^{(2)} \cup \{\gamma^3\} = \{\gamma, \gamma^8, \gamma^3\}$ as independent set for $\mathcal{B}_2$. This yields

$$
\begin{array}{lcll}
C_{11}^{(2)} & = & \{\beta^2(\gamma^3)^2\} & = \{\alpha^{51}\}, \\
C_{12}^{(2)} & = & \gamma^{5\cdot 2} C_{11}^{(2)} \cup \{\beta^2\gamma^{6\cdot 2}\} & = \{\alpha^{16}, \alpha^{30}\}, \\
C_{13}^{(2)} & = & \gamma^{2\cdot 2} C_{12}^{(2)} \cup \{\beta^2\gamma^{3\cdot 2}\} & = \{\alpha^2, \alpha^{16}, \alpha^{51}\}, \\
C_{21}^{(2)} & = & \beta C_{13}^{(2)} \cup \{\beta^4\gamma^{3\cdot 4}\} & = \{\alpha^{38}, \alpha^{52}\alpha^{24}, \alpha^{39}\}, \\
C_{22}^{(2)} & = & \gamma^{5\cdot 4} C_{21}^{(2)} \cup \{\beta^4\gamma^{6\cdot 4}\} & = \{\alpha^{31}, \alpha^{45}, \alpha^{17}, \alpha^{32}, \alpha^{60}\}, \\
C_{23}^{(2)} & = & \gamma^{2\cdot 4} C_{22}^{(2)} \cup \{\beta^4\gamma^{3\cdot 4}\} & = \{\alpha^3, \alpha^{17}, \alpha^{52}, \alpha^4, \alpha^{32}, \alpha^{39}\}, \\
C_{31}^{(2)} & = & \beta^2 C_{23}^{(2)} \cup \{\beta\gamma^3\} & = \{\alpha^{12}, \alpha^{26}, \alpha^{61}, \alpha^{13}, \alpha^{41}, \alpha^{48}, \alpha^{57}\}, \\
C_{32}^{(2)} & = & \gamma^5 C_{31}^{(2)} \cup \{\beta\gamma^6\} & = \{\alpha^{26}, \alpha^{40}, \alpha^{12}, \alpha^{27}, \alpha^{55}, \alpha^{62}, \alpha^8, \alpha^{15}\}, \\
C_{33}^{(2)} & = & \gamma^2 C_{32}^{(2)} \cup \{\beta\gamma^3\} & = \{\alpha^{19}, \alpha^{33}, \alpha^5, \alpha^{20}, \alpha^{48}, \alpha^{55}, \alpha, \alpha^8, \alpha^{57}\}.
\end{array}
$$

Notice that several nonzeros of $\mathcal{C}_3$ appear, ($\alpha^{52}$, $\alpha^{31}$, $\alpha^{45}$, etc.) Again the performance of the Jensen Bound is quite poor: the BCH-bound for $\mathcal{C}_1 \oplus \mathcal{C}_2$ is 10; and this can of course trivially be achieved by shifting.

In this example we saw a code for which the shifting bound is sharp, and the Jensen Bound is even lower than the BCH-bound. A little more could be said about the performance in general of the Jensen Bound if we would know its performance for *all* binary cyclic codes of length 63. We will investigate this by means of Theorem 2.3.2.[3]

We do this as follows: for all possible inner and outer codes we construct as large independent sets as possible under the assumptions of this theorem, and check whether or not the shifting bound is sharp (under these assumptions). If it is, Theorem 2.3.2 guarantees that shifting yields at least as good an estimate on the minimum distance as Equation 1.1 does.

### Inner codes of length 7

[3]See [13] for a computer produced list (based on the list in [9]) of all those codes with true minimum distance, BCH-bound, and the estimate for the minimum distance found with Equation 1.1 for $n = 7$, $N = 9$ ('half' the Jensen Bound). There are 8190 such codes; if equivalent codes are identified , as is done in [13], we find 1554 different codes.

There are 3 minimal cyclic codes of length 7 (over $\mathsf{F}_2$): $\langle\theta_0\rangle$, $\langle\theta_1\rangle$ and $\langle\theta_3\rangle$, with nonzeros 1 respectively $\beta$, $\beta^2$ and $\beta^4$ respectively $\beta^3$, $\beta^6$ and $\beta^5$. Hence outer codes will be codes over $\mathsf{F}_2$ or $\mathsf{F}_8$.

For the codes with idempotents $\theta_0$, $\theta_1$ and $\theta_3$ the BCH-bound is sharp—and can be achieved by shifting with appropriate (in view of the extra assumption) added elements. The codes with idempotents $\theta_0+\theta_1$ and $\theta_0+\theta_3$ have $d = d_{\text{BCH}} = 3$; here too shifting can be applied with appropriate elements, for the sequence of consecutive zeros that yields the BCH-bound is delimited by nonzeros from either of the minimal cyclic codes.

The remaining two codes have minimum distance 2 respectively 1, so we trivially can reach the true minimum distance with independent sets that satisfy the assumptions in Theorem 2.3.2; we denote this as OK.

**Binary outer codes of length 9**

The minimal cyclic codes are: $M_0^-$ with a single nonzero 1 and dimension 1; $M_1^-$ with nonzeros $\gamma$, $\gamma^2$, $\gamma^4$, $\gamma^8$, $\gamma^7$ and $\gamma^5$ and dimension 6; $M_3^-$ with nonzeros $\gamma^3$ and $\gamma^6$ an dimension 2.

Since these codes can be inner codes as well, we will treat them more extensive than necessary at first sight.

$M_0^-$: $d = d_{\text{BCH}} = 9$, so trivially OK.

$M_1^-$: $d = 2$, so trivially OK.

$M_3^-$: $d = 6$, shift as follows: $(\underline{6}) \to (7,\underline{6}) \to (8,7,\underline{6}) \to \cdots \to (2,1,0,8,7,\underline{6})$. Denote this as $\underline{6}(+1)$. OK.

$M_0^- \oplus M_1^-$: $d = 2$; trivially OK.

$M_0^- \oplus M_3^-$: $d = 3$; shift $(\underline{0}) \to (1,\underline{0}) \to (2,1,\underline{0})$ or $(\underline{3}) \to (2,\underline{3}) \to (1,2,\underline{3})$. (Or, in short notation, $\underline{0}(+1)$ or $\underline{3}(-1)$.) OK.

$M_1^- \oplus M_3^-$: $d = 2$; trivially OK.

$M_0^- \oplus M_1^- \oplus M_3^-$: $d = 1$; trivially OK.

**Outer codes of length 9 over $\mathsf{F}_8$**

The minimal cyclic codes are: $M_0^-$ with nonzero 1 and dimension 1; $M_1^-$, $M_2^-$, $M_3^-$, $M_4^-$ with nonzeros $\gamma$ and $\gamma^8$ respectively $\gamma^2$ and $\gamma^7$ respectively $\gamma^3$ and $\gamma^6$ respectively $\gamma^4$ and $\gamma^5$, and all with dimension 2.

All these codes are (equivalent to) BCH-codes; since shifting always reaches the true minimum distance for such codes, viz. by a shift of the form $\underline{i}(+j)$, all codes trivially are OK.

For example:

$M_1^-$: $d = 8$; shift $\underline{8}(+2)$; OK.

$M_2^-$: $d = 8$; shift $\underline{7}(-4)$; OK; equivalent to $M_1^-$.

$M_1^- \oplus M_3^-$: $d = 6$; shift $\underline{3}(+2)$; OK.

$M_0^- \oplus M_1^- \oplus M_4^-$: $d = 5$; shift $\underline{8}(+4)$; OK.

$M_0^- \oplus M_2^- \oplus M_3^- \oplus M_4^-$: $d = 3$; shift $\underline{6}(+2)$; OK.

### Inner codes of length 9

The minimal cyclic codes of length 9 are $\langle\theta_0\rangle$, $\langle\theta_1\rangle$ and $\langle\theta_3\rangle$, with dimensions 1, 6 and 2. Hence the outer codes will be codes over $\mathbb{F}_2$, $\mathbb{F}_{64}$ and $\mathbb{F}_4$.

For all inner codes we can find 'appropriate' independent sets that attain the true minimum distance, see outer codes of length 9 over $\mathbb{F}_2$.

### Binary outer codes of length 7

See inner codes of length 7.

### Outer codes of length 7 over $\mathbb{F}_{64}$

$\mathbb{F}_{64}$ contains all the 7th roots of unity, so we have 7 minimal cyclic codes $M_i^-$, each with one nonzero $\gamma^i$ and dimension 1.

We only give the codes with $d \neq d_{\text{BCH}}$, where we interpret the BCH bound in the narrow sense[4]; we will see that all codes are equivalent to a code with sharp BCH bound (which is the BCH bound in the usual, broader sense).

$M_i^- \oplus M_{i+k}^-$, $0 \leq i \leq 6$, $k \not\equiv 0 \pmod 9$: $d = 6$; shift $\underline{i+k}(+k)$; OK.

$M_i^- \oplus M_{i+1}^- \oplus M_{i+4}^-$, $0 \leq i \leq 6$: $d = 5$; shift $\underline{i}(+3)$; OK.

$M_i^- \oplus M_{i+2}^- \oplus M_{i+4}^-$, $0 \leq i \leq 6$: $d = 5$; shift $\underline{i+4}(+2)$; OK.

$M_i^- \oplus M_{i+2}^- \oplus M_{i+5}^-$, $0 \leq i \leq 6$: $d = 5$; shift $\underline{i+2}(+2)$; OK.

$M_i^- \oplus M_{i+1}^- \oplus M_{i+3}^- \oplus M_{i+4}^-$, $0 \leq i \leq 6$: $d = 4$; shift $\underline{i+3}(+3)$; OK.

$M_i^- \oplus M_{i+1}^- \oplus M_{i+3}^- \oplus M_{i+5}^-$, $0 \leq i \leq 6$: $d = 4$; shift $\underline{i}(+2)$; OK.

$M_i^- \oplus M_{i+1}^- \oplus M_{i+4}^- \oplus M_{i+5}^-$, $0 \leq i \leq 6$: $d = 4$; shift $\underline{i}(+3)$; OK.

All sums of 5 $M_i^-$'s: $d = 3$; if this code has zeros $\gamma^j$ and $\gamma^{j+k}$, then shift $\underline{j-k}(k)$. OK.

[4] I.e., we set the BCH bound to 1 + the number of consecutive zeros of the code; usually we do this for all possible choices of the primitive root. This broader interpretation means that the BCH bound (in the narrow sense) of equivalent codes are taken into account as well.

**Outer codes of length 7 over $\mathbb{F}_4$**

We find the same minimal polynomials as in the binary case. This implies that each code has a binary subcode with the same generator. So the minimum distance of any of these binary subcodes is an upper bound on the minimum distance of the corresponding code over $\mathbb{F}_4$.

Because shifting depends on the zeros only, the shifting bound of a binary subcode is a lower bound on the minimum distance of the corresponding code over $\mathbb{F}_4$. As we have seen under 'Inner codes of length 7', both bounds are equal. This proves that the shifting bound is sharp for the codes over $\mathbb{F}_4$ as well.

**Conclusion**

**Corollary 2.3.4** *For all binary cyclic codes of length 63 shifting yields at least as good a lower bound on the minimum distance as the Jensen Bound does.*

In several cases it will be better (cf. Examples 2.3.1 and 2.1.1), often even the BCH-bound is better (see [9]).

## 2.4 Good binary cyclic codes of length 63

In the preceding section we have seen that shifting is at least as good as the Jensen Bound for all binary cyclic codes of length 63. Since the shifting bound is good for all binary cyclic codes of small length, one might expect it to perform reasonably well for all binary cyclic codes of composite length with only small divisors, compared to the Jensen Bound. In this section we go deeper into this, especially into the relative performances of both bounds for 'good codes'.

Given length and alphabet, a nontrivial code is called 'good' if it satisfies:

1. There are no cyclic codes with both larger minimum distance and larger dimension;
2. There are no cyclic codes of the same minimum distance with larger dimension;
3. There are no cyclic codes of the same dimension with larger minimum distance.

(The first requirement is not superfluous: a [63,5,30] cyclic code satisfies 2 and 3, but does not satisfy 1: there exists a [63,6,32] code, see the computer output in [13].)

First we give, in Table 2.1, a list of all 'good' codes of length 63, (where all equivalent codes are identified with one another), with the dimension $k$, with the true minimum distance $d$, with the BCH-bound $d_{\text{BCH}}$ of the equivalent code where

this bound is maximal[5], with the Jensen Bound $d_{JB}$ and with the shifting bound —together with hints how to find an independent set that yields this estimate— in the column under 'shift'. In this column an asterisk indicates we have used some extra tricks to reach the minimum distance; a $^+$ indicates we have used the parity of the weight of codewords.

In the column '(non)zeros' the (non)zeros of one of these equivalent codes are given, where an 'n' denotes that the nonzeros are given, a 'z' that the zeros are given, and an integer $i$ denotes the cyclotomic coset containing $\alpha^i$.

Notice that for the codes with numbers 8, 20, 21, 23, 26, 29, 30, 35, 36 and 38 the Jensen Bound is odd, while these codes are even weight codes. For code 38 this observation immediately yields the true minimum distance, for the other ones it does not make a lot of difference, for the performance of the Jensen Bound is quite poor in these cases.

In a few cases the shifting bound is not sharp. We have tried to find large independent sets that could be used for shifting with the help of a computer program, see [11], Appendix A.

For the codes 15–19 and 26 this program 'proved' that the indicated independent sets really are the largest possible, and thus that $d_{\text{shift}}$ is equal to the value given in the corresponding example. Except for code 15 however, with some extra tricks (in most cases only concerning the parity of the weight of codewords) it was possible to find the true minimum distance of the code.

The following examples indicate how the shifting bound, as given in Table 2.1, can be reached.

**Example 2.4.1** All of the nonzeros of this code can be used as added elements: if $\alpha^3$ is a zero, see code 6; if $\alpha^9$ is a zero, we can find an independent set of cardinality 24, for the Jensen Bound for this code is 24 (use Corollary 2.3.4); if $\alpha^{13}$ is a zero, notice that the exponents of all the nonzeros of this subcode are a multiple of 3.

Now shift as follows: $(\underline{3}) \rightarrow (0, \underline{3}) \rightarrow (0, \underline{48}, 60) \rightarrow (\underline{6}, 45, 57, 60) \rightarrow (0, \underline{6}, 39, 51, 54) \rightarrow (\underline{12}, 27, 39, 42, 51, 57) \rightarrow (15, 30, 42, 45, \underline{48}, 54, 60) \rightarrow (0, \underline{6}, 15, 21, 27, 30, 39, 45)$. (Or take any independent set of cardinality 8 for the code of length 21 with generator $m_0 m_5 m_7 m_9$ and multiply the exponents by 3 (mod 63); this is how this set was found.)

Notice that we have only shifted over multiples of 3 (i.e., multiplied by $\alpha^{3l}$ for some $l$). Now multiply this set by $\alpha$ (i.e., shift over 1).

The new set consists of zeros of the subcode (with extra zero $\alpha^{13}$) only. If we shift *this* set over multiples of 3, the resulting sets still consist of zeros of the subcode only. So add $\alpha^3$, and start shifting as above. (That is: multiply by $\alpha^{-3}$, add $\alpha^3$; multiply by $\alpha^{-3}$, add $\alpha^{48}$; etc.)

[5]This estimate can be found by shifting for all the equivalent codes!

| | (non)zeros | $k$ | $d$ | $d_{\text{BCH}}$ | $d_{\text{JB}}$ | shift | |
|---|---|---|---|---|---|---|---|
| 1 | n 21 | 2 | 42 | 42 | 42 | 42 | 42(+1); (BCH-code) |
| 2 | n 9 | 3 | 36 | 36 | 36 | 36 | 36(+1); (BCH-code) |
| 3 | n 23 | 6 | 32 | 32 | 32 | 32 | 58(+5); (BCH-code) |
| 4 | n 0, 23 | 7 | 31 | 31 | 27 | 31 | 0(+5); (BCH-code) |
| 5 | n 13, 27 | 9 | 28 | 28 | 28 | 28 | 52(+11); (BCH-code) |
| 6 | n 9, 13 | 9 | 28 | 28 | 18 | 28 | 38(+5); (BCH-code) |
| 7 | n 0, 13, 27 | 10 | 27 | 27 | 27 | 27 | 0(+11); (BCH-code) |
| 8 | n 9, 13, 21 | 11 | 26 | 26 | 9 | 26 | 38(+5); (BCH-code) |
| 9 | n 9, 13, 23 | 15 | 24 | 24 | 16 | 24 | 58(+5); (BCH-code) |
| 10 | n 3, 9, 13 | 15 | 24 | 18 | 18 | 24 | Example 2.4.1 |
| 11 | n 0, 9, 13, 23 | 16 | 23 | 23 | 12 | 23 | 0(+5); (BCH-code) |
| 12 | n 9, 13, 21, 23 | 17 | 22 | 22 | 8 | 22 | 58(+5); (BCH-code) |
| 13 | n 0, 9, 13, 21, 23 | 18 | 21 | 21 | 8 | 21 | 0(+5); (BCH-code) |
| 14 | n 0, 11, 13, 15 | 19 | 19 | 14 | 9 | 19 | Example 2.4.2 |
| 15 | n 11, 13, 27, 31 | 21 | 18 | 12 | 16 | 16 | Corollary 2.3.4 |
| 16 | n 13, 15, 23, 27, 31 | 27 | 16 | 14 | 12 | $16^{+}$ | Example 2.4.3 |
| 17 | n 3, 9, 13, 23, 31 | 27 | 16 | 12 | 14 | $16^{*}$ | Example 2.4.4 |
| 18 | n 0, 13, 15, 23, 27, 31 | 28 | 15 | 13 | 9 | $15^{+}$ | Example 2.4.5 |
| 19 | n 0, 3, 9, 13, 23, 31 | 28 | 15 | 11 | 9 | $15^{*}$ | Example 2.4.6 |
| 20 | n 7, 11, 13, 21, 23, 27 | 29 | 14 | 12 | 7 | 14 | Example 2.4.7 |
| 21 | z 0, 1, 3, 5, 7, 9, 31 | 29 | 14 | 14 | 7 | 14 | BCH-code |
| 22 | z 0, 1, 3, 5, 7, 9, 11 | 29 | 14 | 14 | 6 | 14 | BCH-code |
| 23 | z 0, 1, 5, 7, 11, 15, 27 | 29 | 14 | 12 | 7 | 14 | even wt. subcode of 25 |
| 24 | z 1, 3, 5, 7, 9, 11 | 30 | 13 | 13 | 6 | 13 | BCH-code |
| 25 | z 1, 5, 7, 11, 15, 27 | 30 | 13 | 11 | 7 | 13 | Example 2.4.8 |
| 26 | z 0, 1, 3, 5, 9, 31 | 35 | 12 | 10 | 7 | $12^{+}$ | Example 2.4.9 |
| 27 | z 0, 1, 3, 5, 7, 9 | 35 | 12 | 12 | 6 | 12 | BCH-code |
| 28 | z 1, 3, 5, 7, 9 | 36 | 11 | 11 | 5 | 11 | BCH-code |
| 29 | z 0, 1, 3, 15, 31 | 38 | 10 | 10 | 5 | 10 | BCH-code |
| 30 | z 0, 1, 3, 5, 31 | 38 | 10 | 10 | 7 | 10 | BCH-code |
| 31 | z 0, 1, 3, 5, 7 | 38 | 10 | 10 | 6 | 10 | BCH-code |
| 32 | z 1, 3, 5, 7 | 39 | 9 | 9 | 5 | 9 | BCH-code |
| 33 | z 0, 1, 5, 9, 21 | 45 | 8 | 4 | 4 | 8 | Example 2.4.10 |
| 34 | z 1, 5, 9, 21 | 46 | 7 | 4 | 4 | 7 | Example 2.4.11 |
| 35 | z 0, 1, 31 | 50 | 6 | 6 | 3 | 6 | BCH-code |
| 36 | z 0, 1, 3 | 50 | 6 | 6 | 3 | 6 | BCH-code |
| 37 | z 1, 3 | 51 | 5 | 5 | 3 | 5 | BCH-code |
| 38 | z 0, 1 | 56 | 4 | 4 | 3 | 4 | BCH-code |
| 39 | z 1 | 57 | 3 | 3 | 3 | 3 | BCH-code |

Table 2.1: Good codes of length 63

This provides an independent set of cardinality 16 (with respect to a word in the subcode, with nonzeros $\alpha^3$ and $\alpha^9$). This process can be repeated to yield an independent set of cardinality 24.

So only the case where $\alpha^3$, $\alpha^9$ and $\alpha^{13}$ are nonzeros remains. In this case shift:

(48) → (33, 47) → (24, 39, 53) → (29, 41, 44, 58) → (12, 17, 29, 32, 46) → (0, 6, 29, 34, 46, 49) → (0, 23, 28, 33, 40, 43, 57) → (3, 20, 25, 30, 37, 40, 54, 60) → (4, 10, 27, 32, 33, 37, 44, 47, 61) → (8, 13, 14, 20, 37, 42, 43, 47, 54, 57) → (6, 11, 16, 17, 23, 40, 45, 46, 50, 57, 60) → (1, 3, 8, 11, 20, 25, 30, 31, 36, 37, 54, 59, 60) → (0, 3, 17, 22, 23, 27, 29, 34, 37, 46, 51, 56, 57) → (1, 10, 15, 20, 21, 27, 30, 33, 44, 49, 50, 54, 56, 61) → (0, 5, 8, 17, 23, 27, 28, 33, 34, 37, 40) → (2, 6, 11, 16, 21, 22, 27, 28, 31, 34, 45, 50, 51, 55, 57, 62) → (0, 3, 5, 10, 11, 16, 17, 20, 23, 34, 39, 40, 44, 46, 51, 54, 58) → (0, 5, 8, 10, 15, 16, 21, 22, 24, 25, 28, 39, 44, 45, 49, 51, 56, 59) → (4, 5, 7, 8, 11, 12, 22, 27, 28, 32, 34, 39, 42, 46, 51, 54, 56, 61, 62) → (0, 6, 10, 15, 16, 20, 22, 27, 30, 34, 39, 42, 44, 49, 50, 55, 56, 58, 59, 62) → (0, 1, 6, 7, 11, 16, 17, 21, 23, 28, 31, 35, 40, 43, 45, 50, 51, 56, 57, 59, 60) → (0, 1, 4, 5, 6, 10, 11, 15, 20, 21, 25, 27, 32, 35, 39, 44, 47, 49, 54, 55, 60, 61) → (1, 2, 6, 7, 8, 10, 11, 14, 15, 16, 20, 21, 25, 30, 31, 35, 37, 42, 45, 49, 54, 57, 59) → (0, 1, 5, 6, 10, 11, 15, 17, 22, 25, 29, 34, 37, 39, 44, 45, 49, 50, 51, 53, 54, 57, 58, 59).

Notice that only once an added element is not a zero of $m_3$; both times it is a zero of $m_{13}$. (This makes the remark concerning the subcode with extra zero $\alpha^9$ superfluous.)

**Example 2.4.2** This a is rather hard example: we have to distinguish 8 cases, viz. all possible subcodes with extra zeros from $\{\alpha^{11}, \alpha^{13}, \alpha^{15}\}$. (Whether or not 1 is a zero does not matter: 1 is not used as a zero nor as a nonzero in the independent sets we construct.)

If none of $\alpha^i$, $i = 11, 13, 15$ is a zero, shift as follows:

(13) → (10, 13) → (1, 4, 26) → (2, 13, 24, 62) → (1, 12, 23, 37, 61) → (9, 12, 23, 34, 37, 48) → (3, 6, 17, 28, 31, 39, 42) → (7, 10, 19, 21, 32, 35, 43, 46) → (4, 7, 16, 18, 29, 32, 40, 43, 57) → (8, 10, 11, 21, 24, 32, 35, 49, 59, 62) → (6, 9, 11, 23, 33, 36, 45, 47, 48, 58, 61) → (10, 20, 23, 32, 34, 35, 37, 45, 48, 56, 59, 61) → (4, 7, 9, 21, 31, 34, 37, 43, 45, 46, 48, 56, 59) → (7, 17, 20, 23, 29, 31, 32, 34, 42, 45, 53, 56, 57, 58) → (4, 6, 7, 9, 13, 17, 20, 28, 31, 32, 33, 45, 55, 58, 61) → (5, 7, 8, 10, 14, 18, 19, 21, 29, 32, 33, 34, 46, 56, 59, 62) → (1, 7, 9, 10, 12, 13, 16, 20, 21, 23, 31, 34, 35, 36, 48, 58, 61) → (6, 9, 12, 13, 18, 20, 21, 23, 24, 27, 31, 32, 34, 42, 45, 46, 47, 59) → (1, 4, 5, 6, 13, 18, 28, 31, 34, 35, 40, 42, 43, 45, 46, 49, 53, 54, 56).

If $\alpha^{15}$ and $\alpha^{11}$ both are zeros, shift $52(-1)$; if $\alpha^{15}$ and $\alpha^{13}$ are zeros, shift $11(+5)$; in both cases we find independent sets of cardinality larger than 19.

If all three of them are zeros, trivially $d = 63$. The four remaining cases are somewhat harder, but again we can find independent sets of cardinality 19.

**Example 2.4.3** If $\alpha^{13}$ is a zero, we find $d \geq 16$ by the BCH-bound; if it is a nonzero, shift $(\underline{13}) \rightarrow (12, \underline{13}) \rightarrow (9, 10, \underline{13}) \rightarrow (6, 7, 10, \underline{38}) \rightarrow (5, 6, 9, \underline{13}, 37) \rightarrow (8, 9, 12, 16, 40, \underline{41}) \rightarrow (5, 6, 36, 37, 40, \underline{41}, 44) \rightarrow (17, 18, \underline{19}, 21, 22, 25, 49, 50) \rightarrow (1, 2, 32, 33, 34, 36, 37, \underline{38}, 40) \rightarrow (16, 17, 18, \underline{19}, 20, 21, 22, 24, 48, 49) \rightarrow (4\text{–}10, 12, \underline{13}, 36, 37) \rightarrow (3\text{–}9, 11, 12, \underline{13}, 35, 36) \rightarrow \cdots \rightarrow (0\text{–}6, 8\text{–}12, \underline{13}, 32, 33)$; because 1 is a zero, the minimum weight is even, so we conclude $d \geq 16$.

**Example 2.4.4** Corollary 2.3.4 guarantees the existence of an independent set of cardinality 14, and the computer program could not find a larger set.

We can use a trick however, viz. a theorem due to McEliece (cf. [6, 7]). This theorem states that the weight of every codeword is divisible by $2^{l-1}$ if $l$ is the smallest number of nonzeros required to get product 1.

Since the product of two nonzeros cannot be equal to 1 ($\alpha^i \notin R$ if and only if $\alpha^{-i} \in R$), $l \geq 3$, so $4 \mid d$. Hence $d \geq 16$.

**Example 2.4.5** If we have a word of even weight, 1 is a zero of this word, and $d \geq 16$ by Example 2.4.3. So now take a word of odd weight (i.e., 1 is a nonzero).

If $\alpha^{13}$ is a zero, we find $d \geq 16$ by the BCH-bound; if $\alpha^{13}$ is a nonzero, shift as in Example 2.4.3, only omit the last step.

This yields an independent set of cardinality 14. Since $d$ is odd, we find $d \geq 15$.

**Example 2.4.6** If 1 is a nonzero, we distinguish the two cases: $\alpha^9$ is a zero and $\alpha^9$ is a nonzero. In both cases we may assume $\alpha^{23}$ and $\alpha^{31}$ are nonzeros, for if one of them (or both) is a zero, we find $d \geq 16$ respectively 14 (shift $\underline{58}(+5)$ respectively $\underline{48}(+5)$. In both cases we find independent sets of cardinality 14.

A word of even weight however, is in the subfield subcode (code 17), so we immediately can conclude $d \geq 15$.

**Example 2.4.7** Because of the BCH-bound of the subcodes with zeros $\alpha^7$ and/or $\alpha^{23}$, we may assume that they are nonzeros.

Shift: $(\underline{7}) \rightarrow (6, \underline{7}) \rightarrow (5, 6, \underline{7}) \rightarrow (3, 4, 5, \underline{35}) \rightarrow (30, 31, 32, \underline{46}, 62) \rightarrow (15, 16, 17, \underline{23}, 31, 47) \rightarrow (0, 31, 32, 33, \underline{35}, 39, 47) \rightarrow (1, \underline{28}, 32, 33, 34, 36, 40, 48) \rightarrow (12, \underline{14}, 16, 17, 18, 20, 24, 32, 48) \rightarrow (0, 1, 2, 4, 8, 16, 32, \underline{58}, 59, 61) \rightarrow (1, 2, 3, 5, 9, 17, 33, \underline{58}, 59, 60, 62) \rightarrow (0, 2, 3, 4, 6, 10, 18, 34, \underline{58}, 59, 60, 61) \rightarrow (0, 2, 4, 5, 6, 8, 12, 20, 36, \underline{58}, 60, 61, 62) \rightarrow (1, 2, 3, 4, 6, 8, 9, 10, 12, 16, 24, 40, \underline{58}, 62)$.

**Example 2.4.8** We may assume that $\alpha^{21}$ and $\alpha^{31}$ are nonzeros, for the subcode with extra nonzero $\alpha^{21}$ is code number 19 in Table 2.1; for the code with extra zero $\alpha^{31}$ shift $\underline{0}(+5)$ to find wt $\geq 15$.

Now shift as follows: $(\underline{55}) \rightarrow \cdots \rightarrow (40, 45, 50, \underline{55}) \rightarrow (25, 30, 35, 40, \underline{59}) \rightarrow (1, 30, 35, 40, 45, \underline{47}) \rightarrow (22, 27, 32, 37, 39, \underline{42}, 56) \rightarrow (20, 25, 30, 35, 37, 40, \underline{42}, 54) \rightarrow (17, 22, 27, 32, 34, 37, 39, \underline{47}, 51) \rightarrow (15, 20, 25, 30, 32, 35, 37, 45,$

49, $\underline{55}$) → (1, 5, 11, 34, 39, 44, 49, 51, 54, 56, $\underline{59}$) → (10, 15, 20, 25, 27, 30, 32, 35, 40, $\underline{42}$, 44, 50) → (5, 10, 15, 20, 22, 25, 27, 30, 35, 37, 39, $\underline{42}$, 45).

**Example 2.4.9** If either of $\alpha^7$ or $\alpha^{15}$ is a zero of a word, then the BCH-bound yields $\mathrm{wt}(\boldsymbol{c}) \geq 12$; if none of them is a zero, shift as follows:

($\underline{28}$) → (12, $\underline{28}$) → (8, 24, $\underline{56}$) → (8, $\underline{39}$, 40, 55) → (0, 16, 47, 48, $\underline{49}$) → (0, 31, 32, 33, $\underline{39}$, 47) → (0, 1, 2, 8, 16, 32, $\underline{60}$) → (1, 2, 3, 9, 17, 33, $\underline{60}$, 61) → (2, 3, 4, 10, 18, 34, $\underline{60}$, 61, 62) → (0, 1, 4, 5, 6, 12, 20, 36, $\underline{60}$, 62) → (1, 3, 4, 5, 8, 9, 10, 16, 24, 40, $\underline{60}$);

we find $d \geq 11$ and $d$ even (for 1 is a zero), so $d \geq 12$.

**Example 2.4.10** If $\alpha^3$ is a zero, then the BCH-bound yields $\mathrm{wt}(\mathbf{c}) \geq 8$, if it is a nonzero, shift ($\underline{3}$) → (17, $\underline{33}$) → (2, $\underline{6}$, 18) → (5, $\underline{6}$, 9, 21) → (1, 2, 5, $\underline{6}$, 17) → (4, 5, $\underline{6}$, 8, 9, 20) → (16, 17, 18, 20, 21, $\underline{24}$, 32) → (0, 1, 2, 4, 5, $\underline{6}$, 8, 16).

**Example 2.4.11** As Example 2.4.10; only omit the last step.

In the table we can see a few things:

- The BCH-bound is better than the Jensen Bound 28 times, they are equal nine times, (of which they are sharp six times), the Jensen Bound is better only twice.
- The Jensen Bound is only six times sharp[6], and in all cases the BCH-bound is as well. Moreover all these codes have dimension or codimension (= length minus dimension) at most 7. For the other codes the performance of the Jensen Bound often is quite poor.
- Shifting alone already reaches the true minimum distance 33 times; the parity of the weight of codewords yields the true minimum distance another three times, and twice an extra trick suffices. Only one code remains; here shifting falls 2 short of it only: we find $d \geq 16$ instead of 18 for code 15.

## 2.5 A criterion on when the Jensen Bound is sharp

In this section we give the announced criterion on when the Jensen Bound is sharp. This criterion will also be of some interest in view of the judgement of the performance of the Jensen Bound.

**Lemma 2.5.1** *If, for some $l$, $1 \leq l \leq v$, the following holds:*

[6]with the help of the parity of the weight of the code (code 38) and the 'trick' of Ex. 2.4.4 we find two more cases

1. $R(\mathcal{B}_i) \subseteq R(\mathcal{B}_l)$*for all* $i < l$;

2. *There is a* $q$*-ary word of minimum weight in* $\mathcal{B}_l$;

*then there is a word of weight* $d_{1l}d_{2l}$.

**Proof:** Let $\boldsymbol{b}$ be a $q$-ary word of minimum weight in $\mathcal{B}_l$. Since all the $\mathcal{B}_i$ with $i < l$ have $\mathcal{B}_l$ as a subcode, $\boldsymbol{b}$ is in all these codes as well. Let $\sum_{i=1}^{l} a_i(x)$ be a word of minimum weight $d_{1l}$ in $\langle \theta_1 + \cdots + \theta_l \rangle$. Notice that the $a_i$ represent ($q$-ary) words in the corresponding $\langle \theta_i \rangle$. Now the word

$$\boldsymbol{c} = \sum_{s=1}^{l} \Psi_s(a_s(\beta_s)\boldsymbol{b}) = \sum_{s=1}^{l} \Psi_s\left(a_s(\beta_s) \sum_{j=0}^{N-1} b_j y^j\right) = \sum_{s=1}^{l} a_s(x) \sum_{j=0}^{N-1} b_j y^j$$

has $\mathrm{wt}(\boldsymbol{b})$ nonzero columns, (viz. those columns where $\boldsymbol{b}$ has a nonzero entry), while each column is of the form $b_j \sum a_s(x)$, that is, each nonzero column has weight $\mathrm{wt}(\sum a_s) = d_{1l}$. So $\mathrm{wt}(\boldsymbol{c}) = d_{1l}d_{2l}$. □

This lemma itself is not very helpful; with an extra observation it becomes slightly more helpful.

In Section 2.2 we saw that — without changing the code itself — a different choice of the $\beta_s$ yields a different representation of a cyclic code as a 2-D cyclic code with different, but equivalent outer codes, and the same Jensen Bound. We use this idea to extend the use of the lemma to a larger class of codes, and to be able to say something about when the Jensen Bound is sharp.

It is not difficult to prove that, if we take $\beta_s = \beta^{sq^t}$ instead of $\beta_s = \beta^s$, we find outer code $\mathcal{B}'_s = \bigoplus_i M^-_{iq^t}$ instead of $\mathcal{B}_s = \bigoplus_i M^-_i$. With the appropriate maps the codes $\bigoplus_s \langle \theta_s \rangle \square \mathcal{B}_s$ and $\bigoplus_s \langle \theta_s \rangle \square \mathcal{B}'_s$ represent the same cyclic code; and moreover they have the same value in Equation 1.1. From this it follows that it suffices to require the existence of integers $t_s$, $1 \leq s \leq l$, such that the corresponding $\mathcal{B}'_s$ satisfy requirement 1 in the lemma, and the existence of a $q$-ary word of weight $d_{1l}$, to find a word of weight $d_{1l}d_{2l}$. This proves the following theorem.

**Theorem 2.5.2** *If there is an integer* $l$, $1 \leq l \leq v$, *such that:*

1. *There are integers* $t_s$, $1 \leq s \leq l$ *such that the codes* $\mathcal{B}'_s$ *as described above satisfy* $R(\mathcal{B}'_s) \subseteq R(\mathcal{B}'_l)$ *for all* $s < l$;

2. *There is a* $q$*-ary word of minimum weight in* $\mathcal{B}_s$;

3. $d_{1i}d_{2i} \geq d_{1l}d_{2l}$ *for all* $i$;

*then the Jensen Bound is sharp.*

Now consider a code $C$ that satisfies the conditions of Theorem 2.5.2, and a second code $C'$ with the same inner codes and outer codes $\mathcal{B}'_s$ of the same dimension as the corresponding $\mathcal{B}$, and minimum distance such that the value in Equation 1.1 does not change. If we do not have that $\mathcal{B}'_s \cong \mathcal{B}_s$ for all $s$, we can not apply the lemma, so the Jensen Bound need not be sharp for $C'$. Hence $C'$ might have larger minimum distance.

Additionally we possibly can take $\mathcal{B}'_s$ with larger dimension than the $\mathcal{B}_s$ for $s \neq l$, i.e., add some extra nonzeros, while condition 3. remains satisfied. Hence there may be codes, possibly of larger dimension, for which the Jensen Bound is not sharp, that is, with larger minimum distance. We give an example.

**Example 2.5.1** Let $C$ be the binary cyclic code of length 63 with generator polynomial $m_0 m_1 m_5 m_7 m_9 m_{23} m_{31}$. Then, as a $7 \times 9$ 2-D cyclic code, $C = \langle\theta_3\rangle\Box(M_0^- \oplus M_2^- \oplus M_3^-) \bigoplus \langle\theta_1\rangle\Box(M_3^- \oplus M_4^-) \bigoplus \langle\theta_0\rangle\Box M_3^-$, so in this case Equation 1.1 yields $d \geq \min\{4 \cdot 3, 2 \cdot 6, 1 \cdot 6\} = 6$. $C$ satisfies the conditions of Theorem 2.5.2, and indeed the Jensen Bound is sharp: $d = 6$.

If we take $\mathcal{B}'_0 = \mathcal{B}_0$, $\mathcal{B}'_1 = M_2^- \oplus M_3^-$ and $\mathcal{B}'_3 = M_0^- \oplus M_2^- \oplus M_4^-$ we find code 22 from Table 2.1. Equation 1.1 still yields $d \geq 6$, for the case $9 \times 7$ it yields $d \geq 5$. As we have seen however, $C'$ has minimum distance 14. Since this was a 'good' code, we cannot add extra nonzeros without 'losing some minimum distance'.

The observations made after Theorem 2.5.2 are not restricted to codes with sharp Jensen Bound that satisfy the conditions of this lemma, as the next example shows.

**Example 2.5.2** Let $C$ be the binary cyclic code of length 63 with generator polynomial $m_1 m_5 m_7 m_9 m_{11} m_{21} m_{23} m_{31}$. Here $\mathcal{B}_3 = M_0^- \oplus M_2^- \oplus M_3^-$, $\mathcal{B}_1 = M_3^-$ and $\mathcal{B}_0 = M_0^-$. Equation 1.1 yields $d \geq \min\{4 \cdot 3, 2 \cdot 6, 1 \cdot 9\} = 9$, which is the true minimum distance.

If we take $\mathcal{B}'_1 = M_2^-$ and $\mathcal{B}'_3 = M_0^- \oplus M_2^- \oplus M_4^-$, we find a code with the same Jensen Bound, which is taken for the same value of $l$: Equation 1.1 yields $d \geq \min\{4 \cdot 3, 2 \cdot 8, 1 \cdot 9\} = 9$. ($\mathcal{B}'_1$ has larger minimum distance than $\mathcal{B}$, but this has no effect on the value in Equation 1.1.) For the $9 \times 7$ 2-D cyclic code we find $d \geq 6$ by Equation 1.1. The true minimum distance however is 15.

If we add $M_3^-$ to $\mathcal{B}'_1$, we find code 18 from Table 2.1, still with the same Jensen Bound and minimum distance, but with dimension 28 instead of 22.

We can do this the other way around as well: first add $M_2^-$ to $\mathcal{B}_1$, (after which we find a code with dimension 28 and sharp Jensen Bound of 9); then change $\mathcal{B}_3$ to $\mathcal{B}'_3$ (as before; $\mathcal{B}'_1$ already is as before by adding $M_2^-$).

These examples and observations give rise to the impression that the Jensen Bound does not perform too well for good codes. Inspection of 'Bijlage 3' (the computer output mentioned before) shows that Equation 1.1 for the case $7 \times 9$

('half' the Jensen Bound, and probably in general the best half) is only incidentally sharp for the best codes of given dimension, while it is quite often for the worst ones. Together with the performance for the good codes of length 63 (see Table 2.1) and the observations above, this leads us to the suspicion that the Jensen Bound does, in general, not perform too well for good codes, and reasonably well for bad ones.

## 2.6 Other lengths; conclusions

The observations made after Theorem 2.5.2 are restricted to codes such that we can always choose an other outer code, inequivalent to the given outer code.

Now consider codes of length $nN = 69$. We will see that for $n = 3$, $N = 23$ the Jensen Bound is exact for all codes but one, exactly 'because' we cannot choose these (inequivalent) outer codes.

For $n = 3$, the outer codes must be codes over $\mathbb{F}_2$ or $\mathbf{F}_4$. Over both fields, we find the same minimal idempotents. This immediately shows that requirement 2. from Theorem 2.5.2 is satisfied. Since the code generated by $M_1^-$ is equivalent to the code generated by $M_{-1}^-$, we see that requirement 1 is not satisfied only if 1 is a zero of $\mathcal{B}_1$ but not a zero of $\mathcal{B}_2$. By inspection of the few remaining codes for which requirement 1 does not hold, we find that the only code[7] for which the Jensen Bound need not be sharp is the code $\langle\theta_0\rangle \square M_1^- \oplus \langle\theta_1\rangle \square M_0^-$, for which we find $d \geq \min\{3 \cdot 8, 1 \cdot 23\} = 23$. Since this code is an even weight code, this implies $d \geq 24$; the true minimum distance for this code is 24.

We construct a table again compiling all 'good' codes of length 69; see Table 2.2 (cf. the table in [10]).

As we have seen, the Jensen Bound is sharp for all codes in the table.

Comparison with Table 2.1 however, reveals that none of these codes, except possibly codes 1 and 10, are as good as the good codes of length 63. (Either there is a code of the same dimension and larger minimum distance, or there is a code of the same minimum distance, but with larger dimension.)

So this good performance of the Jensen Bound is not contradictory to our suspicion that the Jensen Bound does not do too well for good codes.

Furthermore, the usefulness of the remarks made in the previous section may be restricted if $x^n - 1$ and/or $y^N - 1$ have only few irreducible divisors (over the appropriate fields). Apart from $nN = 69$, this also holds for the three next smallest odd composite lengths, viz. 75, 77 and 85.

First, consider the good codes of length 75, see Table 2.3. (see [10] for all the codes of length 75.)

From the table we see that the Jensen Bound is exact ten times; with the help of the parity of minimum distance we find the true minimum distance another

[7] up to equivalence

| | zeros | $k$ | $d$ | $d_{\text{BCH}}$ |
|---|---|---|---|---|
| 1 | 0, 1, 3, 5, 15 | 2 | 46 | 46 |
| 2 | 0, 1, 3, 5 | 13 | 24 | 18 |
| 3 | 1, 3, 5 | 14 | 21 | 15 |
| 4 | 3, 5, 15, 23 | 23 | 16 | 9 |
| 5 | 1, 3, 15 | 25 | 14 | 7 |
| 6 | 0, 1, 3 | 35 | 12 | 6 |
| 7 | 1, 3 | 36 | 11 | 5 |
| 8 | 0, 1 | 46 | 6 | 4 |
| 9 | 15, 23 | 56 | 4 | 3 |
| 10 | 23 | 67 | 2 | 2 |

Table 2.2: Good codes of length 69

| | (non)zeros | $k$ | $d$ | $d_{\text{BCH}}$ | $d_{\text{JB}}$ |
|---|---|---|---|---|---|
| 1 | n 25 | 2 | 50 | 50 | 50 |
| 2 | n 5 | 4 | 40 | 40 | 40 |
| 3 | n 0, 5 | 5 | 35 | 35 | 25 |
| 4 | n 15, 25 | 6 | 30 | 30 | 25 |
| 5 | n 25, 35 | 6 | 30 | 30 | 30 |
| 6 | n 0, 25, 35 | 7 | 25 | 25 | 25 |
| 7 | n 15, 25, 35 | 10 | 20 | 20 | 15 |
| 8 | n 0, 15, 25, 35 | 11 | 15 | 15 | 15 |
| 9 | n 5, 15, 25, 35 | 14 | 10 | 10 | 10 |
| 10 | z 0, 3, 7, 25 | 32 | 8 | 7 | 8 |
| 11 | z 3, 7, 25 | 33 | 7 | 7 | 5 |
| 12 | z 0, 1, 3 | 34 | 6 | 6 | 6 |
| 13 | z 0, 1, 7 | 34 | 6 | 6 | 5 |
| 14 | z 1, 3 | 35 | 5 | 5 | 5 |
| 15 | z 0, 1 | 54 | 4 | 4 | 3 |
| 16 | z 1 | 55 | 3 | 3 | 2 |
| 17 | z 25 | 73 | 2 | 2 | 2 |

Table 2.3: Good codes of length 75

| | zeros | $k$ | $d$ | $d_{\text{BCH}}$ | $d_{\text{JB}}$ |
|---|---|---|---|---|---|
| 1 | 0, 1, 3, 7, 33 | 3 | 44 | 44 | 44 |
| 2 | 1, 3, 7, 33 | 4 | 33 | 33 | 33 |
| 3 | 0, 1, 3, 7 | 6 | 22 | 22 | 22 |
| 4 | 0, 1, 3 | 16 | 14 | 14 | 11 |
| 5 | 1, 7, 33 | 34 | 8 | 6 | 8 |
| 6 | 3, 11 | 44 | 6 | 5 | 6 |
| 7 | 7, 33 | 64 | 4 | 3 | 4 |
| 8 | 11 | 74 | 2 | 2 | 2 |

Table 2.4: Good codes of length 77

three times. This is, compared to the performance of the Jensen Bound for codes of length 63, relatively good. The BCH bound performs better though: this bound is sharp 16 times; for the only code where it is not, use of the parity immediately yields the true minimum distance as well.

Comparison with the good codes of length 63 in Table 2.1 again shows that the good codes of length 63 are better than those of length 75, (possibly with the exception of codes 1, 2 and 17), so again these results do not contradict our suspicion.

Next, consider the good codes of length 77. Again we find, in the case $7 \times 11$, that the outer codes have binary subcodes with the same generator, so again we might expect relatively good performance of the Jensen Bound. But, just as for the codes of length 69, the good codes of length 77 are not as good as the codes of length 63, see Table 2.4, (again see [10]).

Again these results do not contradict our suspicion.

In [3] however, four codes of length 85 are given, all of which are 'good', (again cf. [10]). These codes seem to be about as good as codes of length 91 and 93.

We will consider these five codes more closely now.

1. The first one has parameters $[85, 37, 17]$, and is the only code (up to equivalence) with these parameters.

2. The second one, a $[85, 41, 16]$-code, is one of two, nonequivalent codes with these parameters. For the code that is not given in [3], the Jensen Bound is at most 10, (and at least 7): as a $5 \times 17$ 2-D cyclic code, this code equals $\langle m_1 m_{21} m_{15} m_{17} m_{29} m_{37} \rangle = \langle \theta_0 \rangle \square (M_0^- \oplus M_3^-) \bigoplus \langle \theta_1 \rangle \square (M_2^- \oplus M_5^- \oplus M_6^- \oplus M_8^-)$.

   The outer code $\mathcal{B}_0$ is a QR code of length 17; it has minimum distance 6. (This can be seen by considering the code $\langle \theta_1 \rangle \square \mathcal{B}_0$ of length 51 with

this code as its only outer code: this is code 125 in [6], and has minimum distance 12. Since all columns of this code are words of $\langle \theta_1 \rangle$, all columns (of all words) have weight 2, so $d(\mathcal{B}_0) = 6$.)

The other outer code has BCH bound 7, and minimum distance at most 10 (by the Singleton Bound). Now Equation 1.1 immediately yields the stated lower bound.

The case $17 \times 5$ provides $d \geq 4$.

3. This code has parameters $[85, 45, 14]$, and is — again up to equivalence — the only code with these parameters.

4. The fourth code is one of the five nonequivalent codes with parameters $[85, 49, 12]$. For all four codes not listed in [3], the Jensen Bound is at most 11. (Analogous to what we found under 2.; once the BCH bound of $\mathcal{B}_1$ is 11, and is sharp (Singleton Bound), so the Jensen Bound is equal to 11 in that case. Furthermore, in all cases the same outer code $\mathcal{B}_0$ as under 2. is found.)

5. The last code of length 85, given in [3], is a $[85, 53, 10]$-code. There are four codes with these parameters; the one given in [3] is equivalent to the code with generator $m_1 m_3 m_5 m_{15}$, given in [10].

   - The first one that is not given is a nice example of a difficulty that sometimes — especially with codes that consist of a small number of $\mathcal{C}_i$ — arises when calculating the Jensen Bound. This code $\mathcal{C} = \langle m_3 m_5 m_7 m_{15} \rangle = \langle \theta_1 \rangle \square (M_0^- \oplus \cdots \oplus M_4^- \oplus M_7^- \oplus M_8^-) \bigoplus \langle \theta_0 \rangle \square M_0^-$, so $d \geq \min\{2 \cdot d(\mathcal{B}_1), 1 \cdot 17\} = 2 \cdot d(\mathcal{B}_1)$.

     Now $d(\mathcal{B}_1) \geq 4$ by the Hartmann-Tzeng bound, (and shifting does not improve this). To find the true minimum distance of this outer code, however, is not much easier than finding it for $\mathcal{C}$ itself, for the number of words in $\mathcal{B}_1$ is half the number of words in $\mathcal{C}$, but the outer code is a code over $\mathsf{F}_{16}$.

     So if we do not want to do the extra work involved in calculating the minimum distance of $\mathcal{B}_1$ — which is quite logical, for it might yield less information than the calculation of $d(\mathcal{C})$ itself[8]— we find $d \geq 8$.

   - For the second one, $\langle m_5 m_7 m_9 m_{13} \rangle$, we find the true minimum distance 5 of $d(\mathcal{B}_1)$ by shifting, and $\mathcal{B}_0$ is the same QR code we saw before. So $d \geq 6$ by Equation 1.1 as for the first one. (Again the case $17 \times 5$ does not improve this.)

[8] we might find that the true minimum distance is 4; then we do not know anything more than before doing all this, while doing the same thing for $\mathcal{C}$ itself could provide the true minimum distance of $\mathcal{C}$

- The third code that is not given in [3], has Jensen Bound 6 as well, (this time $d(\mathcal{B}_1) = 5$ by the BCH bound).

This leads us to the following formulation of our suspicion:

**Conclusion:** In general, the Jensen Bound does not do too well for good codes, it does reasonably well for 'bad' ones; probably the performance is better for lengths $nN$ that satisfy some of the following requirements.

- $x^n - 1$ and/or $y^N - 1$ have only a small number of primitive divisors, (over $\mathsf{F}_q$ respectively the fields $F_s$).
- All codes in $F_sG_y$ have a subcode with the same generator in $\mathsf{F}_qG_y$.

(For specific codes the Jensen Bound of course may be good (or even sharp), even if it does not do well for codes of this length in general.)

# Chapter 3

# Use of the 2-D Cyclic Structure of Cyclic Codes

## 3.1 Introduction

In Section 3.2 a more or less new method of estimating the minimum distance of a cyclic code is presented. The basic idea is quite simple, and based on two observations. Firstly, shifting seems to perform quite well in general, but it is an elaborate method, especially for longer codes: in fact we must shift for all subcodes of the code of which we want to estimate the minimum distance, and it is quite hard to see how we should perform shifting to get optimal results. Often we can skip a lot of those subcodes: in Example 2.4.2 we could ignore whether or not 1 is a zero of a word of minimum weight.

Secondly, the Jensen Bound seems to perform not so well. However, it mostly is easier to calculate, and — more important — it provides information on some of the subcodes: in Example 2.4.1 we saw, with help of the Jensen Bound, that all the subcodes with extra zero $\alpha^9$ have weight at least 24.

In Section 3.3, finally, some good codes of length 2047 are constructed.

## 3.2 The basic idea

The idea is to do the following: calculate the Jensen Bound, but instead of upper bounding the weight of the words of $C_1 \oplus \cdots \oplus C_l$ with nonzero component in $C_l$ by $d_{1l}d_{2l}$, use the maximum of this estimate and the shifting bound or any other useful bound for this code. Furthermore we can, especially for smaller (inner and/or outer) codes, use the fact that not all symbols in the alphabet of the outer code yield the same (minimum) weight of columns; this provides a better estimate than the Jensen Bound itself. This last idea will prove to be very useful in some cases.

We can formulate the idea as follows:

$$d \geq \min\{d_{\text{est}}(\mathcal{D}_l)\} \mid 1 \leq l \leq v\}, \tag{3.1}$$

where $\mathcal{D}_l = \{\mathbf{c} \in \bigoplus_{i=1}^{l} \mathcal{C}_i \mid \mathbf{c}_l \neq 0\}$ and $d_{\text{est}}$ is the best estimate we can find for the minimum distance of the code, using the 2-D cyclic structure of the code.

We look at some codes of length 65. The next example is treated in [6] as well, but there a special trick is needed; with use of the Jensen Bound this trick becomes superfluous — at least in this case.

**Example 3.2.1** Let $\mathcal{C} = \langle m_1 m_3 m_5 \rangle$, binary and of length 65. This code provides a nice illustration of the idea.

As a $(5 \times 13)$ 2-D cyclic code $\mathcal{C} = \langle\theta_1\rangle\Box(M_0^- \oplus M_4^- \oplus M_8^-) \bigoplus \langle\theta_0\rangle\Box M_0^-$, yielding $d \geq \min\{d(\mathcal{C}_1), 1 \cdot 13\}$. Since $\mathcal{C}_1$ is the even weight subcode of $\mathcal{C}$, and since $d_{\text{BCH}}(\mathcal{C}_1) = 14$, we immediately find $d \geq 13$, which is the true minimum distance.

The same can be done by principles 1) and 3) in [6]; these principles state: for a code of length 65 with generator $g$ the following holds:

1) if $m_5 \mid g$ then $d$ even or $d \geq 13$, ($g$ the generator of the code)

3) if $d$ even then the even weight subcode has the same minimum distance.

It is not hard to see that we can either derive these principles from the 2-D cyclic structure of the code, or, as we did in this example, use this structure itself to obtain the same result.

The next example is treated in [6] as well.

**Example 3.2.2** Let $\mathcal{C}$ be the binary cyclic code of length 65 with generator $g = m_1 m_5$. As a $5 \times 13$ 2-D cyclic code $\mathcal{C}$ equals $\langle\theta_1\rangle\Box(M_0^- \oplus M_2^- \oplus M_4^- \oplus M_8^-) \bigoplus \langle\theta_0\rangle\Box M_0^-$, yielding $d \geq \min\{2d(\mathcal{B}_1), 1 \cdot 13\}$. So $d \geq 13$ or all words of minimum weight are in $\mathcal{C}_1$ (which is the even weight subcode).

Now the Hartmann-Tzeng bound shows that $d \geq 7$, for $\{\alpha^i \mid i = -2, -1, 15, 16, 32, 33, 49, 50, 1, 2\} = \{\alpha^i \mid i = -2, -1\} \cdot \{\alpha^i \mid i = 0, 17, 34, 51, 68\} \subset R$, that $d \geq 7$. Because $d$ is even, we conclude $d \geq 8$, which is exact.

Remark: in [6] this is proved in a different way (by principles 1) and 3), as quoted above); it can be proved in yet another way: either shift[1] $\underline{0}(+5)$ (to find $d \geq 13$) or assume 1 is a zero of the codewords of minimum weight. All three methods give exactly the same result.

We will now prove a lemma, that will enable us to treat some other codes of length 65 (among which some quite hard ones).

[1] So in fact this is not such a good example to indicate the usefulness of (3.1), for we can do this by shifting alone!

**Lemma 3.2.1** *Let $\theta_1$ be the primitive idempotent of the binary even weight code of length 5, and $\mathcal{B}_1$ a cyclic code over $\mathsf{F}_{16}$. Then the minimum distance of a code $\mathcal{C} = \langle\theta_1\rangle\Box\mathcal{B}_1$ is equal to $2\cdot d(\mathcal{B}_1)$ if and only if there is a word $\boldsymbol{b}$ of minimum weight in $\mathcal{B}_1$ such that none of its symbols $c_i$ is in $\{1, \beta, \ldots, \beta^4\}$.*

**Proof:** Obviously there are only five words of weight 4 in $\theta_1$, all other words have weight 2. In fact the five 'heavy' words are $x^i\theta_1$, $i = 0, \ldots, 4$. In Section 1.3 we already saw that $\psi_1(1) = \theta_1$ and $\psi_1(\beta_1 a) = x\psi_1(a)$. From this it immediately follows that a letter $\beta^i$, $i = 0, \ldots, 4$, results in a column of weight 4, and all other letters (field elements of $\mathsf{F}_{16}$) give rise to a column of weight 2. □

A corollary of this lemma is that the weight of a word $\psi_1(\boldsymbol{b})$ in $\langle\theta_1\rangle\Box\mathcal{B}_1$ is $4\cdot|\{i \mid b_i^5 = 1\}| + 2\cdot|\{i \mid b_i^5 \neq 0, 1\}|$. With the aid of this we can treat the next example. (This code appeared (as Example 57) in [6] as well.)

**Example 3.2.3** Let $\mathcal{C}$ be the binary cyclic code of length 65 with generator $m_1m_5m_7$. For $n = 5$, $N = 13$, we find $\mathcal{C} = \langle\theta_1\rangle\Box(M_0^- \oplus M_2^- \oplus M_8^-)\bigoplus\langle\theta_0\rangle\Box M_0^-$. This yields $d \geq \min\{2\cdot 5, 1\cdot 13\} = 10$.

We will show now that all words of minimum weight in $\mathcal{B}_1$ have at least one coordinate in $\{1, \ldots, \beta^4\}$. Since the minimum distance of $\mathcal{B}_1$ is 5 (by the BCH bound), this implies $d \geq 12$: by the lemma this inequality holds for all words in the outer code of minimum weight 5; trivially it holds for all words in the outer code of weight $\geq 6$.

Let $\xi$ be a generator of $\mathsf{F}_{16}$, and denote the trace function $\mathsf{F}_{16} \to \mathsf{F}_4$ by Tr, i.e., $\mathrm{Tr}(x) = x + x^4$ for all $x$ in $\mathsf{F}_{16}$. Furthermore denote the vector $(\mathrm{Tr}(c_0), \mathrm{Tr}(c_1), \ldots, \mathrm{Tr}(c_{12}))$ by $\mathrm{Tr}(c_0, c_1, \ldots, c_{12})$.

The zeros of $\mathcal{B}_1$ are $\gamma$, $\gamma^3$, $\gamma^4$, $\gamma^9$, $\gamma^{10}$ and $\gamma^{12}$. Notice that $\mathcal{B}_1$ is a QR code. Since $y$ is a zero of $\mathcal{B}_1$ if and only if $y^4$ is a zero, $b(y) = \sum_i b_i y^i$ is a codeword if and only if $b'(y) = \sum_i b_i^4 y^i$ is a codeword ($b(y) = 0$ if and only if $b'(y^4) = 0$).

So if $\boldsymbol{b}$ is a codeword, then $\mathrm{Tr}(\boldsymbol{b})$ is a codeword as well. Now the trace of a word is in the subfield subcode (over $\mathsf{F}_4$) with the same generator. Since we can take a scalar multiple of $\boldsymbol{b}$ to make sure its trace is not equal to $\mathbf{0}$, the subfield subcode has the same minimum distance. (This part of the argument appears as Theorem 9 and its proof in [6].)

Let $\boldsymbol{b}$ be a scalar multiple of an arbitrary word of minimum weight in $\mathcal{B}_1$, such that $\boldsymbol{b}$ has at least one coordinate equal to 1. Since $\mathrm{Tr}(1) = 0$, we find that $\mathrm{wt}(\mathrm{Tr}(\boldsymbol{b})) < \mathrm{wt}(\boldsymbol{b})$, so $\mathrm{Tr}(\boldsymbol{b}) = \mathbf{0}$. Hence, for all $i$, $b_i \in \{0, 1, \xi^5, \xi^{10}\}$, which is the set of field elements (of $\mathsf{F}_{16}$) with zero trace.

Define $a_i = |\{j \mid b_j = \xi^i\}|$ for all $i$. Now suppose only one of $a_0$, $a_5$ and $a_{10}$ not equal to zero. Then we find a binary word of weight 5, a contradiction, as the only binary word with zeros $\gamma$ and $\gamma^4$ is the all-one word $\mathbf{1}$. So at most one of $a_0$, $a_5$ and $a_{10}$ is zero.

Suppose exactly one of the $a_{5i}$ is zero, say $a_{10}$. Then there are two nonequivalent possibilities: $a_0 = 1$ and $a_0 = 2$; all other cases are equivalent to one of these

two (by taking a scalar multiple) or can be treated analogously (by renaming the elements of $\mathbb{F}_4$, see below).

We take a scalar multiple of $b$ such that all five coordinates are $\omega$ or $\omega^2$. Then write $b(y) = \omega f_1(y) + \omega^2 f_2(y)$, where the $f_i$ are polynomials over $\mathbb{F}_2$, and either $\mathrm{wt}(f_1) = 1$ and $\mathrm{wt}(f_2) = 4$, or $\mathrm{wt}(f_1) = 2$ and $\mathrm{wt}(f_2) = 3$, corresponding to $a_0 = 1$ respectively 2.

Now $\bar{b}(y) = \omega^2 f_1(y) + \omega f_2(y)$ is in the QR code with defining set $\{\gamma^i \mid i = 2, 5, 6, 7, 8, 11\}$. (This follows from the fact that $(\bar{b}(y))^2 = (b(y^2))$.)

But then $b(y) \cdot \bar{b}(y)$ is in the repetition code of length 13. Since obviously 1 is not a zero of $b$, nor of $\bar{b}$, this product must be the all-one word.

However, $b(y)\bar{b}(y) = f_1^2(y) + f_2^2(y) + f_1(y)f_2(y)$. In the case $a_0 = 1$ we find that this is the sum of $1 + 4 + 4 = 9$ powers of $y$, ($f_1^2$ contributes one power of $y$; $f_2^2$ four, as does $f_1 f_2$); for $a_0 = 2$ we find $2 + 3 + 6 = 11$ powers of $y$. So in both cases we cannot have the all-one word, a contradiction.

This proves that in all words of minimum weight exactly three different nonzero symbols occur; these symbols constitute one of the sets $\{\xi^i, \xi^{5+i}, \xi^{10+i}\}$, $0 \leq i < 5$. In other words: all words of minimum weight are scalar multiples of words of minimum weight in the subfield subcode. Since all these sets contain a power of $\beta$, viz. $\xi^{3j}$, $0 \leq j < 5$, we conclude $d \geq 12$.

The code in the next example contains the same outer code $\mathcal{B}_1$ again, and we can use the knowledge we have just gained to deal with this code as well. (It is given as an example in [6] as well.)

**Example 3.2.4** Let $\mathcal{C} = \langle m_0 m_1 m_7 \rangle = \langle \theta_0 \rangle \square M_1^- \oplus \langle \theta_1 \rangle \square \mathcal{B}_1$ in the case $5 \times 13$. Theorem 1.5.1 yields $d \geq \min\{5 \cdot 2, 1 \cdot 5\} = 5$. We immediately see that $d \geq 6$, as $\mathcal{C}$ is an even weight code.

In terms of the matrix representation this is easy to explain as well: $\mathcal{C}_0$ obviously consists of all matrices with an even number of all-one columns, while $\mathcal{C}_1$ consists of columns of weight 2 and/or 4 (viz. words of $\langle \theta_1 \rangle$) on the support of $b_1$. So if we add a word $c_0 = \Psi_0(b_0)$ in $\mathcal{C}_0$ and a word $c_1 = \Psi_1(b_1)$ in $\mathcal{C}_1$, we can get only columns of weight 1 on the (whole) support of $b_1$, only if $\mathrm{wt}(b_1)$ is even, which implies $d \geq 6$.

This means we can try to do the same thing for this code as for the code in the previous example.

Let the number of 'heavy letters' in $b_1$ be $\bar{a} = |\{j \mid b_{1j}^5 = 1\}|$. Now there are two kinds of candidates for a word $c = c_0 + c_1$ in $\mathcal{C}$ of weight less than 8:

- $\mathrm{wt}(b_1) = 5$. The minimum weight for $\mathrm{wt}(b_0) = 2$ is at least 8 and words with $\mathrm{wt}(b_0) \geq 6$ trivially yield a word of weight at least 10, so we need only consider the case $\mathrm{wt}(b_0) = 4$.

- $\mathrm{wt}(b_1) = 6$. Then, if $\bar{a}$ is even, the minimum weight is assumed for $\bar{a}$ columns of weight 1, and $6 - \bar{a}$ columns of weight 2. If $\bar{a}$ is odd, then

minimum weight is assumed if we have a word in $\boldsymbol{b}_0$ with weight $\bar{a}+1$.[2] So, we find

$$d \geq \begin{cases} \bar{a}+2(6-\bar{a}) & \text{if } \bar{a} \text{ is even,} \\ \bar{a}+3+2(6-\bar{a}-1) & \text{if } \bar{a} \text{ is odd.} \end{cases}$$

We first treat the first candidate. In the previous example we saw that the nonzero $b_{1j}$ take all values in one of the sets $\{\xi^i, \xi^{5+i}, \xi^{10+i}\}$ for exactly one $i$. Therefore at least two $b_{1i}$ are not a 5th root of unity, whence $\mathrm{wt}(\boldsymbol{c}) \geq (5-\bar{a}-1)\cdot 2 + 1\cdot 3 + \bar{a}\cdot 1 \geq 8$.

The second candidate is even easier to deal with. In order to prove $d \geq 8$, we must show that $\bar{a} \neq 6$. A word of weight 6 with six 'heavy' letters, however, must have at least one of those letters occur at least twice, and at most five times (because, if it would occur six times, we would have a binary word of weight 6, but these do not exist). Now take a multiple, such that 1 occurs (at least) twice; the trace of this word has nonzero weight at most 4, which is a contradiction.
**Conclusion:** $d \geq 8$.

We can do something more: it can be proved that all words of weight 8 in this code have a component $\boldsymbol{c}_1 = \Psi_1(\boldsymbol{b}_1)$, with $\mathrm{wt}(\boldsymbol{b}_1) = 5$ (and $\mathrm{wt}(\boldsymbol{b}_0) = 4$). This will also yield some information that can be used in the next example as well.

To prove this statement, we must prove that all words with $\mathrm{wt}(\boldsymbol{b}_1) = 6$ have weight at least 9; in other words, we must show that $\bar{a} < 4$.

To do this, we use the trace of codewords again; we distinguish three cases.

- $\mathrm{Tr}(\boldsymbol{b}_1) = \mathbf{0}$: In the same way as in the previous example, we can show that in $\boldsymbol{b}_1$ only symbols from one of the sets $\{\xi^j, \xi^{5+j}, \xi^{10+j}\}$ occur. We prove now that there are no words of weight 6 in $\mathcal{B}_1$ that have only two different nonzero symbols. We do this as follows.

  Again trivially no words with only one kind of nonzero symbol exist; to prove that there are no words with two kinds of different nonzero symbols, we distinguish three cases, depending on the value of $a_0$, which we assume (w.l.o.g.) to be the smallest of the two nonzero $a_l$.

  For the case $a_0 = 3$ we need some extra notation. Define $R_0 = \{1, 3, 4, 9, 10, 12\}$ and $R_1 = \{2, 5, 6, 7, 8, 11\}$, and $f(l) = \sum_{i \in R_0} \gamma^{il}$; calculate modulo 13.

  Obviously $f(0) = 0$, and $f(l)^4 = f(l)$ for all $l$. Therefore, for all $l \neq 0$, $f(l) = \omega^i$, $i = 1, 2$. ($f(l) = 0$ or 1 would imply the existence of a binary word of weight 6 in the code (over $\mathsf{F}_4$) with defining set $R_0$ or $R_1$.) Finally, $f(l) = f(m)$ implies that $l$ and $m$ are in the same $R_i$, or $l = m = 0$. Assume $f(l) = \omega$ if and only if $l \in R_1$; the other case goes completely analogously.

[2] Weight $\bar{a} - 1$ provides a word of larger weight.

Consider the sum $S(\boldsymbol{b}_1) = \sum_{i \in R_0} b_1(\gamma^i)$. Since $\boldsymbol{b}_1$ is a codeword, obviously $S(\boldsymbol{b}_1) = 0$. On the other hand, if $b_1(y) = \sum_{j=0}^{12} b_j y^j$, we see that also $S(\boldsymbol{b}_1) = \sum_{j=0}^{12} \sum_{i \in R_0} b_j \gamma^{ij} = \sum_{j=0}^{12} b_j f(j)$. The fact that this sum is 0, together with the fact that $f(j) = \omega$ or $\omega^2$, is enough to find a contradiction in the case $a_0 = 1$ and 3.[3]

1. $a_0 = 1$: Then the other nonzero $a_j$, say $a_5$, equals 5. We can write $\boldsymbol{b}_1$ as $b_1(y) = 1 + \omega(y^a + y^b + y^c + y^d + y^e)$. Then $S(\boldsymbol{b}_1) = \omega(f(a) + f(b) + \cdots + f(e)) = 0$. This leads to a contradiction, for the sum of an odd number of $\omega$'s and $\omega^2$'s cannot be equal to 0.

   (We can use the same argument as in the previous example as well: since 1 is a zero of both $\boldsymbol{b}_1$ and $\bar{\boldsymbol{b}}_1$, their product must be equal to the zero word $\mathbf{0}$. However, we find that $b_1 \cdot \bar{b_1}$ consists of $1 + 5 + 5 = 11$ powers of $y$; so this product cannot be equal to $\mathbf{0}$.)

2. $a_0 = 2$: In this case write $\boldsymbol{b}' = \omega \boldsymbol{b}$; now $\boldsymbol{b}'$ only has coordinates $\omega$ and $\omega^2$. So write $b'(y) = \omega f_1(y) + \omega^2 f_2(y)$, with $\mathrm{wt}(f_1) = 2$ and $\mathrm{wt}(f_2) = 4$. We find that $\bar{b}(y) = \omega^2 f_1(y) + \omega f_2(y)$ is in the QR code with defining set $\{\gamma^i \mid i \in R_1\} \cup \{1\}$, (analogous to the argument in the previous example).

   Since in this case both $b$ and $\bar{b}$ have a zero 1, their product must be the zero word. In this case we find 14 (not necessarily different) powers of $y$: $b \cdot \bar{b} = f_1^2 + f_2^2 + f_1 f_2$. Write (w.lo.g.) $f_1(y) = 1 + y^i$, and $f_2(y) = y^a + y^b + y^c + y^d$. ($0$, $i$, $a$, $\ldots$, $d$ all are different.) Then we have the following powers of $y$: $y^j$, $j = 0$, $2i$, $2a$, $\ldots$, $2d$, $a + 0$, $\ldots$, $d + 0$, $a + i$, $\ldots$, $d + i$.

   Since the product of $b$ and $\bar{b}$ is the zero polynomial, all the powers of $y$ that occur in the product, must occur an even number of times. We will prove that this is impossible.

   Assume, w.l.o.g.[4], that $i = 1$. Since $y^0$ does occur, there must be a second exponent 0. Obviously this can only be one of $a + 1, \ldots, d + 1$, say $a$; so $a = -1$.

   Furthermore, since 2 occurs as an exponent, it must occur at least once more. so we must have (w.l.o.g.) that $b = 2$. Finally, since $-2$ occurs as an exponent, it must occur once more, so (w.l.o.g.) $c = -3$. Now $y^d$, $y^{2d}$ and $y^{d+1}$ must cancel 5 different powers of $y$,[5] which clearly is impossible.

[3] In fact all cases that are treated with the '$b \cdot \bar{b}$-method' can be done this way as well. In most cases this is quite tedious though.

[4] Multiplication does not influence the number of incidences, and this is the only thing we consider here.

[5] viz. $y^j$, $j = -1, -3, -6, 3, 4$

3. $a_0 = 3$. Then write $b_1(y) = 1 + y^a + y^b + \omega(y^c + y^d + y^e)$. Now

$$S(b_1(y)) = f(a) + f(b) + \omega(f(c) + f(d) + f(e)) = 0,$$

from which it follows that $f(a) = 1 + f(b)$. From $S(y^{-a}b_1(y)) = 0$ and $S(y^{-b}b_1(y)) = 0$ we obtain (analogously) $f(a) = 1 + f(b-a)$ and $f(b) = f(a-b)$, implying $f(a) = f(b)$. Again we find a contradiction.

We find that all of $a_0$, $a_5$ and $a_{10}$ are at least one. Thus the only kind of words with $\bar{a} \geq 4$ is a word with 2 symbols occurring once, and one symbol occurring four times.

Suppose such a word exists, then assume without loss of generality that $b_1(y) = 1 + \omega y^a + \omega^2(y^b + y^c + y^d + y^e)$. Then $S(b_1(y)) = \omega f(a) + \omega^2(f(b) + \cdots + f(e)) = 0$. As a consequence $f(a) = \omega$. From $S(y^{-a}b_1(y)) = f(-a) + \omega^2(f(b-a) + \cdots + f(e-a)) = 0$ however, we find $f(a) = \omega^2$, so such a word $\boldsymbol{b}_1$ does not exist.

Thus we have proved not only that $\bar{a} < 4$, but also that this holds for all multiples of $\boldsymbol{b}_1$.

- $\mathrm{wt}(\mathrm{Tr}(\boldsymbol{b}_1)) = 5$: In this case all symbols of $\boldsymbol{b}_1$ are different, for two equal symbols would imply $0 < \mathrm{wt}(\boldsymbol{b}_1 - \xi^l \mathrm{Tr}(\boldsymbol{b}_1)) < 5$, for some value of $l$, (viz. the value of $l$ satisfying $\xi^l \mathrm{Tr}(\eta) = \eta$, where $\eta$ is the symbol occurring twice. This weight cannot be 0 because the symbol with zero trace always contributes a nonzero symbol to $\boldsymbol{b}_1 - \xi^l \mathrm{Tr}(\boldsymbol{b}_1))$.

  Now suppose $\beta$, $\beta^2$, $\beta^3$ and $\beta^4$ all are symbols of $\boldsymbol{b}_1$. Call the last symbol with nonzero trace $\eta$, and the symbol with zero trace $\zeta$. Now $\eta = \xi^{\pm 5}\beta^i$ for some $i$. Since both 1 and $\xi^{\pm 5}$ have zero trace, but all of $\beta^{-i}\beta^j$

  for $j \neq i$, as well as $\beta^{-i}\zeta$, have nonzero trace, we see that this implies $\mathrm{wt}(\mathrm{Tr}(\beta^{-i}\boldsymbol{b}_1)) = 4$, a contradiction.

  Next, suppose that 1 and three other 5th roots of unity occur as a symbol in $\boldsymbol{b}_1$. By taking a multiple $\beta^i \boldsymbol{b}_1$, we obtain (for some value of $i$) a word with $\beta$, $\beta^2$, $\beta^3$ and $\beta^4$ as symbols. Such a word cannot exist: we can apply the argument of the previous paragraph for this word as well (only in this case there might be two elements with nonzero trace; this is irrelevant to the argument though).

  Thus we see that in $\boldsymbol{b}_1$ at most three 5th roots of unity occur. Moreover, again we see that the same property holds for all scalar multiples of $\boldsymbol{b}_1$

- $\mathrm{wt}(\mathrm{Tr}(\boldsymbol{b}_1)) = 6$: One of the scalar multiples of such a word has a trace of weight either 5 or 0. These words and their multiples have been dealt with in the previous cases.

All this proves that $\bar{a} < 4$, whence $\mathrm{wt}(\boldsymbol{c}) \geq 10$ for all words with $\mathrm{wt}(\boldsymbol{b}_1) \geq 6$.

In the next example a sharp lower bound on the minimum distance of the considered code is given; to the knowledge of the author this has not been done before. (The true minimum distance has been found by computer search.)

**Example 3.2.5** Let $C = \langle m_0 m_1 m_5 m_7 m_{13} \rangle = \langle \theta_1 \rangle \Box (M_2^- \oplus M_8^-)$, $(5 \times 13)$.

The outer code has minimum distance at least 6, which can be proved by shifting. (Shift $(\underline{5}) \rightarrow (4, \underline{5}) \rightarrow (3, 4, \underline{7}) \rightarrow (0, 1, 4, \underline{5}) \rightarrow (0, 3, 4, \underline{6}, 12) \rightarrow (0, 1, 3, \underline{6}, 9, 10)$.)

That the true minimum distance is in fact 6 can be shown by considering the code of length 39 with generator $m_1 m_3 m_{13}$. As its outer code this code has the subfield subcode of $\mathcal{B}_1 = M_2^- \oplus M_8^-$ over $\mathbb{F}_4$. The code of length 39 has minimum distance 12, whereas the Jensen Bound proves $d \geq 2d(M_2^- \oplus M_8^-)$. Since the inner code (of the code of length 39) only has words of weight 2, we conclude $d(M_2^- \oplus M_8^-) = 6$.[6]

We first consider the words in $\mathcal{B}_1$ of weight 6. By applying the trace function to words of minimum weight again, we find that these words are scalar multiples of words in the subfield subcode. So again words of minimum weight have coefficients from exactly one of the sets $\{\xi^j, \xi^{5+j}, \xi^{10+j}\}$, $0 \leq j < 5$.

We apply the same argument as before to these words: if only one kind of nonzero coordinate occurs, we find a binary word of weight 6, which is impossible; if two kinds of nonzero coordinates occur, use the fact that the sum of all coordinates of a codeword is zero, which implies that the parity of the number of occurrences of the three different nonzero coordinates is equal. Then we are in the case '$\mathrm{wt}(\mathrm{Tr}(\boldsymbol{b}_1)) = 0$, $a_0 = 2$' of the previous example; we have seen there that no such word exists.

Hence each word has exactly 3 different nonzero symbols from exactly one of the sets $\{\xi^j, \xi^{5+j}, \xi^{10+j}\}$, $0 \leq j < 5$.

Since the sum of the coordinates of a codeword of $\mathcal{B}_1$ is 0, two 5th roots of unity are coordinates of each codeword. The weight of the related word in $C$ is $2 \cdot 4 + 4 \cdot 2 = 16$.

Finally, consider a word $\boldsymbol{b}$ of weight 7 in $\mathcal{B}_1$. In $\mathrm{Tr}(\boldsymbol{b})$ there is at least one symbol that occurs at least twice. So a suitable multiple of $\boldsymbol{b}$ has a trace of weight at most 5, i.e., it has zero trace. This shows that the symbols of $\boldsymbol{b}$ all are in the same set $\{\xi^i, \xi^{5+i}, \xi^{10+i}\}$. It follows that $\boldsymbol{b}$ has at least one heavy symbol, implying $wt(\Psi_1(\boldsymbol{b})) \geq 1 \cdot 4 + 6 \cdot 2 = 16$.

**Conclusion:** $d \geq 16$.

[6] Of course this observation makes shifting for the outer code superfluous; for the code of length 39 we must find another way (other than the Jensen Bound) to find the minimum distance. In [6] this is done; cf. code 47 and Example 25.

The same trick can be used for the last code of length 65 for which no proof of the minimum distance existed (to the knowledge of the author).

**Example 3.2.6** Let $C = \langle m_0 m_1 m_7 m_{13} \rangle = \langle \theta_0 \rangle \Box M_1^- \oplus \langle \theta_1 \rangle \Box (M_2^- \oplus M_8^-)$. Equation 1.1 yields $d \geq \min\{5 \cdot 2, 1 \cdot 6\} = 6$.

In the matrix representation $C_0$ consists of all matrices consisting of an even number of all-one columns. Since a word of weight 6 in $\mathcal{B}_1$ has, as we have seen in the previous examples, exactly two 'heavy' letters, we find $\mathrm{wt}(\boldsymbol{c}) \geq 2 \cdot 1 + 4 \cdot 2 = 10$ for words $\boldsymbol{c}$ in $C$ we obtain from a word in $\mathcal{B}_1$ of weight 6.

Next, let $\boldsymbol{b}$ be a word of weight 7 in $\mathcal{B}_1$. Then, if we denote the number of times a 5th root of unity occurs as a symbol of $\boldsymbol{b}$ as $\bar{a} = \mid \{j \mid b_j^5 = 1\} \mid$ again,

$$\mathrm{wt}(\boldsymbol{c}) \geq \begin{cases} \bar{a} + 2(7 - \bar{a}) & \text{if } \bar{a} \text{ is even;} \\ \bar{a} + 3 + 2(7 - \bar{a} - 1) & \text{if } \bar{a} \text{ odd and } \neq 7; \\ 10 & \text{if } \bar{a} = 7. \end{cases}$$

So in order to prove $d \geq 10$, we must show that $\bar{a} \neq 6$.

Suppose that $\bar{a} = 6$. Then there is a 5th root of unity, w.l.o.g. 1, occurring at least twice and at most five times[7] as a symbol. But then $1 < \mathrm{wt}(\mathrm{Tr}(\boldsymbol{b})) \leq 5$, a contradiction. Hence $\bar{a} \neq 6$.

Finally, consider a word $\boldsymbol{b}$ of weight 8 in $\mathcal{B}_1$. The only possibility for a word with weight less than 10 is one with eight heavy symbols. So, suppose $\boldsymbol{b}$ has eight 5th roots of unity as symbols. Then one of these symbols, w.l.o.g. 1, must occur at least twice. Then the weight of the trace must be 6. This leads us to a contradiction, for in that case the trace has two 1's, two $\omega$'s and two $\omega^2$'s, and there are no 5th roots of unity with trace 1. Hence at most seven 5th roots of unity occur as a symbol in $\boldsymbol{b}$, so words of weight 8 in $\mathcal{B}_1$ give rise to words of weight at least 10. (With the same technique we can even prove that a word of weight 8 has at most six heavy letters.)

Words of weight $\geq 9$ in $\mathcal{B}_1$ trivially yield words of weight 10 in $C$.

**Conclusion:** $d \geq 10$.

[7] because the sum of the symbols is 0

## 3.3 Construction of some binary cyclic codes

### 3.3.1 Length 2047

Good cyclic codes can be constructed using Theorem 1.4.4 and good cyclic inner and outer codes, though not every appropriate set of good inner and outer codes will provide a good (2-D) cyclic code. More 'conditions' can be derived from Sections 2.3 and 2.4.

One of the first good codes that come to mind is the binary Golay code. We will try to use its minimal components as inner codes. We describe the binary Golay code as the cyclic code of length 23 with idempotent $\theta_0 + \theta_1$. There is only one minimal idempotent other than $\theta_0$ and $\theta_1$; the corresponding code $\langle \theta_{-1} \rangle$ is isomorphic to $\langle \theta_1 \rangle$.

First, we construct $\mathcal{C}_1$. $\langle \theta_1 \rangle$ has minimum distance 8 and dimension 11. Therefore, $\mathcal{B}_1$ will be a code over $\mathbb{F}_{2^{11}}$. We will take an MDS-cyclic code for $\mathcal{B}_1$. This is guaranteed if $\mathbb{F}_{2^{11}}$ contains all $N$th roots of unity and if $\mathcal{B}_1$ is a BCH-code. Therefore, we take $N$ such that $2047 \equiv 0 \pmod{N}$. Since $\gcd(23, N)$ must be equal to 1, this implies $N = 89$. Let $\mathcal{B}_1$ be a BCH-code of length 89 and dimension $K$ over $\mathbb{F}_{2^{11}}$. $\mathcal{B}_1$ has minimum distance $90 - K$.

The outer code $\mathcal{B}_0$ is a *binary* code of length 89. Let $\mathcal{B}_0$ be the repetition code; then it has dimension 1 and minimum distance 89.

Now Equation 1.1 yields

$$d \geq \min\{8 \cdot (90 - K), 7 \cdot 89\} = \begin{cases} 720 - 8K & \text{if } K \geq 13 \\ 623 & \text{if } K < 13. \end{cases}$$

So we find a class of codes $[2047,\ 11K + 1,\ \geq 720 - 8K]$ for $K \geq 13$ and a class of codes $[2047, 11K + 1, \geq 623]$ for $K < 13$.

For this last class the exact minimum distance is 623 if 1 is not a zero of $\mathcal{B}_1$, for in that case the code satisfies the conditions of Lemma 2.5.2. From this it follows that in that case the only interesting code of this class, if any, is the code [2047, 133, 623] ($K = 12$).

If 1 is a zero, we can not apply Lemma 2.5.2, so, with an intelligent choice of $\mathcal{B}_1$, the codes with $K \leq 12$ may have larger minimum distance than the Jensen Bound guarantees.

The same applies for the codes with $K > 12$; in this case $l$ (from the lemma) is equal to 1, so the only requirement of the lemma that is not a priori satisfied is the second one: we do not know if there is a binary word of minimum weight (and in any case we can choose the outer code $\mathcal{B}_1$ such that there is no such word). Hence all of the codes with $K \geq 12$ may have larger minimum distance than $720 - K$ (again assuming an intelligent choice of the outer code).

However, comparison with known BCH codes (cf. [4]) show that the codes with $K = 20$ to 34 are better than previously known codes. Jensen, in [3], gives codes with the same parameters; probably the same codes.

### 3.3.2 Length 4095

Using code 19 from Table 2.1, and outer codes of length 65, we can construct a code of length 4095, superior to those given in [4]: this code has parameters $[4095, 421, 1008]$; Jensen (in [3]) however, gives an even better code, with parameters $[4095, 456, 1008]$.

# Bibliography


[1] E. R. Berlekamp and J. Justesen, 'Some long cyclic linear binary codes are not so bad', *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 351–356, 1974.

[2] E. L. Blokh and V. V. Zyablov, 'Coding of Generalized Concatenated Codes', *Probl. Inform. Transm.*, vol. 10, no. 3, pp. 218–222, 1974.

[3] J. M. Jensen, 'The Concatenated Structure of Cyclic and Abelian Codes', *IEEE Trans. Inform. Theory*, vol. IT-31, no. 6, pp. 788–793, 1985.

[4] T. Kasami and N. Tokura, 'Some Remarks on BCH Bounds and Minimum Weights of Binary Primitive BCH Codes', *IEEE Trans. Inform. Theory*, vol. IT-15, no. 3, 1969.

[5] J. H. van Lint, *Introduction to Coding Theory*, New York-Heidelberg-Berlin: Springer-Verlag 1982.

[6] J. H. van Lint and R. M. Wilson, 'On the Minimum Distance of Cyclic Codes', *IEEE Trans. Inform. Theory*, vol. IT-32, no. 1, pp. 23–40, 1986.

[7] R. J. McEliece, 'Weight Congruences for $p$-ary Cyclic Codes', *Discrete Math.*, vol. 3, pp. 177–192, 1972.

[8] F. J. McWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, New York: North-Holland, 1981.

[9] W. W. Peterson and E. J. Weldon, *Error Correcting Codes*, (2nd ed.), Cambridge, Mass.: MIT Press, 1972.

[10] G. Promhouse and S. E. Tavares, 'The Minimum Distance of Binary Cyclic Codes of Odd Lengths from 69 to 99', *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 438–442, July 1978.

[11] P. J. N. de Rooij, *On the Use of the 2-D Cyclic Structure of Cyclic Codes*, Master's Thesis, Eindhoven University of Technology, 1989.

[12] P. J. N. de Rooij and J. H. van Lint, 'More on the Minimum Distance of Cyclic Codes', *IEEE Trans. Inform. Theory*, vol. IT-37, no. 1, pp. 187–189, January 1991.

[13] M. Schlüper, *The Concatenated Structure of Cyclic and Abelian Codes*, report, Eindhoven University of Technology, 1986.

[14] L. M. G. M. Tolhuizen, *On the Optimal Use and the Construction of Linear Block Codes*, Masters Thesis, Eindhoven University of Technology, 1986.